IT Score for Security & Risk Management

Sample Report Excerpt

Gartner®

Disclaimer

Confidentiality and Intellectual Property
These materials have been prepared by Gartner Inc. and/or its affiliates ("Gartner") for the exclusive and individual use of our clients. These materials contain valuable confidential and proprietary information belonging to Gartner, and they may not be shared with any third party (including independent contractors and consultants) without the prior approval of Gartner. Gartner retains any and all intellectual property rights in these materials and requires retention of the copyright mark on all pages reproduced.

Legal Caveat
Gartner is not able to guarantee the accuracy of the information or analysis contained in these materials. Furthermore, Gartner is not engaged in rendering legal, accounting, or any other professional services. Gartner specifically disclaims liability for any damages, claims, or losses that may arise from a) any errors or omissions in these materials, whether caused by Gartner or its sources, or reliance upon any recommendation made by Gartner.

Disclaimer
Unless otherwise set forth in your Service Description or marked expressly for external use, these items may be downloaded and customized for internal noncommercial use by the Client. The items contained in this report may not be repackaged or resold. Gartner makes no representations or warranties as to the suitability of this report for any particular purpose, and disclaims all liability for any damage or loss, whether direct, consequential, incidental or special, arising out of the use of or inability to use this material or the information provided herein.

Gartner®

Report Roadmap

Introduction	Gartner Score Overview and Model
Executive Summary	Key Findings
Path to Maturity	Next Steps on the Path to Increased Maturity
Next Steps	How Can Gartner Help
Appendix	Additional Pathways, Detailed Data, and Methodology

Gartner®

Gartner Score Overview

Introduction to Gartner Score

Gartner Score enables organizations to improve functional performance by assessing their performance across a broad set of functional activities. The diagnostic measures two primary dimensions: maturity and importance.

IT Score for Security & Risk Management covers 30 functional activities across 7 functional objectives.

Explanation of Scales

Maturity

Measured on a scale ranging from 1 (low) to 5 (high), maturity measures how advanced an organization's development is in a functional activity relative to Gartner's best practice research. Maturity scores are refined with a (+) or (–) to indicate intermediate levels of maturity.

Maturity level descriptions are dependent on the specific activity being assessed.

Importance

As measured by survey participants on a scale ranging from 1 (not important) to 5 (most important), importance measures how important each function activity is to the overall effectiveness of your function in meeting its business objectives.

Value	Description
1	Not Important
2	Somewhat Important
3	Important
4	Very Important
5	Most Important

Research Methodology

Activity Priority Index (API) is used to identify the activities that should be prioritized for improving maturity. It is defined as the average gap between importance and maturity and is computed for each activity and then weighted by its average importance.

Gartner®

Report Roadmap

Introduction	Gartner Score Overview and Model
Executive Summary	Key Findings
Path to Maturity	Next Steps on the Path to Increased Maturity
Next Steps	How Can Gartner Help
Appendix	Additional Pathways, Detailed Data, and Methodology

Gartner®

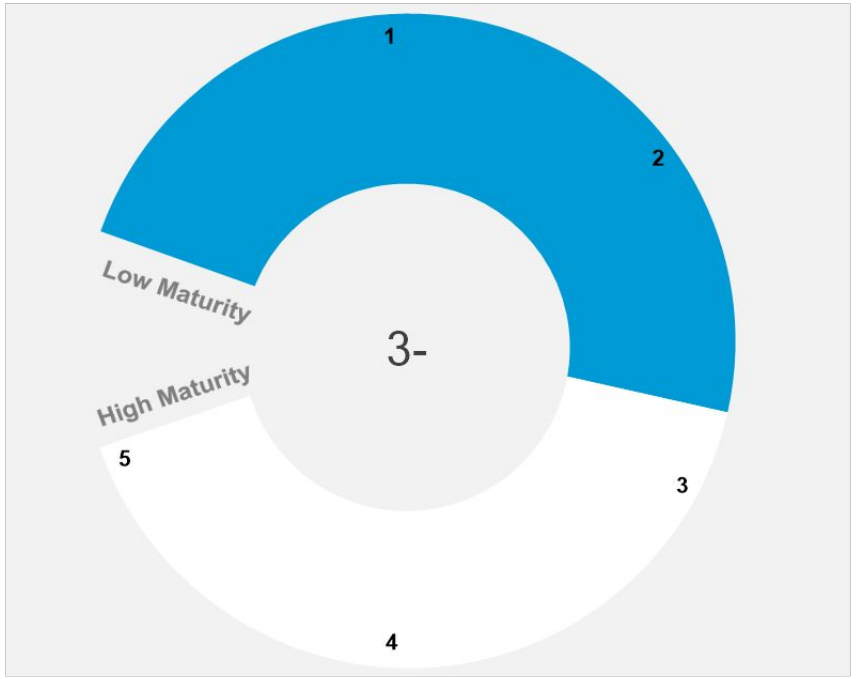
What is Your Overall Maturity?

Overall functional maturity is the average maturity of all activities assessed.

• Measured on a scale ranging from 1 (low) to 5 (high), maturity is an organization's performance relative to Gartner's best practice research. Maturity scores are refined with a (+) or (-) to indicate intermediate levels of maturity.

• The next page has individual maturity scores for each activity, allowing you to quickly identify strengths and opportunities for improving maturity.

Overall Maturity



Benchmark not yet available

Number of respondents for this assessment = 2

Gartner®

How Mature Are Your Functional Activities?

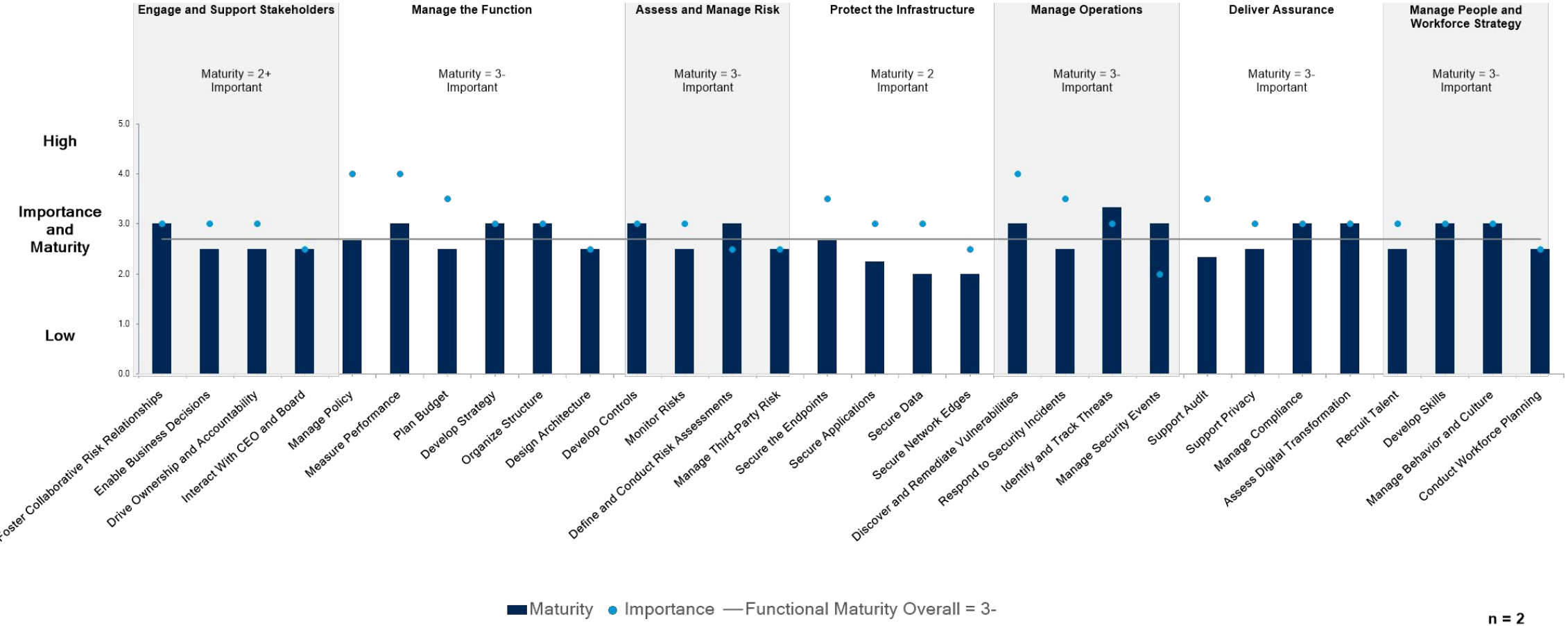
Engage and Support Stakeholders 2+	Manage the Function 3-	Assess and Manage Risk 3-	Protect the Infrastructure 2	Manage Operations 3-	Deliver Assurance 3-	Manage People and Workforce Strategy 3-
Interact with CEO and Board 2+	Develop Strategy 3	Define and Conduct Risk Assessments 3	Secure Network Edges 2	Discover and Remediate Vulnerabilities 3	Support Privacy 2+	Conduct Workforce Planning 2+
Foster Collaborative Risk Relationships 3	Plan Budget 2+	Develop Controls 3	Secure the Endpoints 3-	Manage Security Events 3	Manage Compliance 3	Recruit Talent 2+
Enable Business Decisions 2+	Organize Structure 3	Manage Third-Party Risk 2+	Secure Applications 2	Respond to Security Incidents 2+	Support Audit 2+	Develop Skills 3
Drive Ownership and Accountability 2+	Design Architecture 2+	Monitor Risks 2+	Secure Data 2	Identify and Track Threats 3+	Assess Digital Transformation 3	Manage Behavior and Culture 3
	Manage Policy 3-					
	Measure Performance 3					

Legend High Maturity | Medium Maturity | Low Maturity | Not Assessed | n = 2

Maturity: Measured on a scale ranging from 1 (Low) to 5 (High), maturity measures how advanced an organization's development is in a functional activity relative to Gartner's best practice research. Maturity scores are refined with a (+) or (-) to indicate intermediate levels of maturity.

Gartner®

How Do Maturity and Importance Compare?



n = 2

Lowest Maturity
- Secure Data
- Secure Network Edges
- Secure Applications
- Support Audit

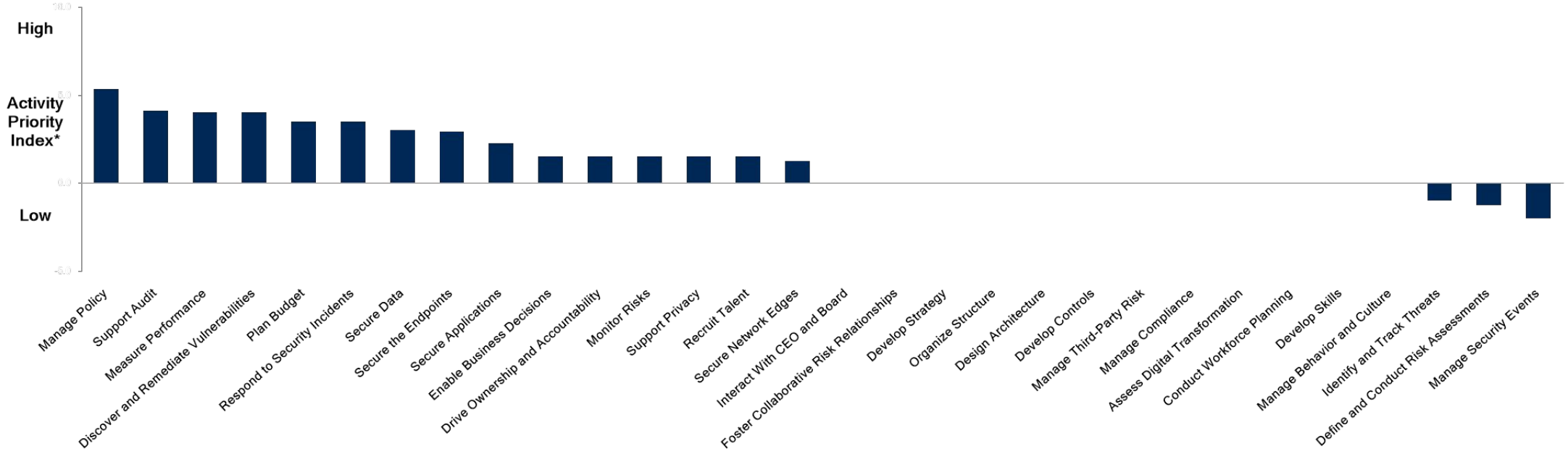
Highest Importance
- Manage Policy
- Measure Performance
- Discover and Remediate Vulnerabilities
- Plan Budget

Importance: Measured on a scale ranging from 1 (Not Important) to 5 (Most Important), Importance measures how important each functional activity is to the overall effectiveness of your function in meeting its business objectives. Please refer to appendix section for scores.

Gartner®

What are the High Priority Areas for Your Function?

The Activity Priority Index identifies where the function is less mature in activities of greater importance.



n = 2

Highest Priority
- Manage Policy
- Support Audit
- Measure Performance and more activities

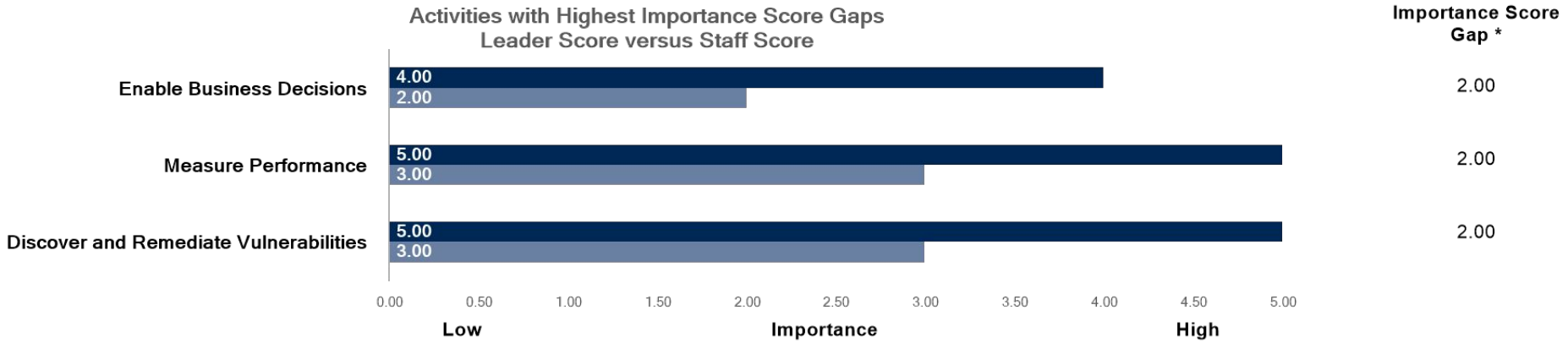
Lowest Priority
- Manage Security Events
- Define and Conduct Risk Assessments
- Identify and Track Threats

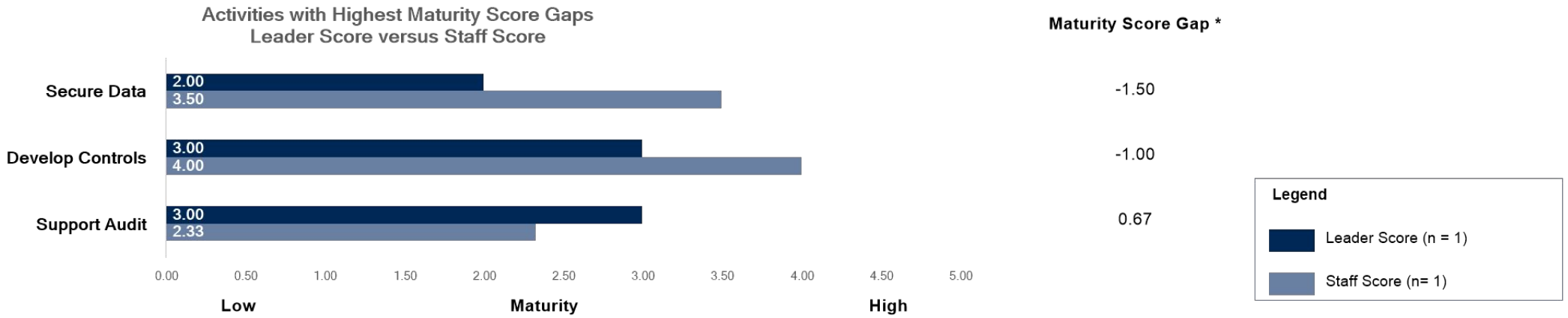
*** Activity Priority Index: Activity Priority Index (API) for an activity is computed as average importance minus maturity multiplied by its average importance. A higher Activity Priority Index score indicates a greater priority to the organization.**

Gartner®

Do We Have Team Consensus on Maturity and Importance?

Presented below are the differences between the leader's and staff's maturity and importance scores for the activities with the highest score gaps.





*** Importance & Maturity Gap: An activity's importance and maturity gaps are the functional head's importance/maturity score minus the staff's average importance/maturity score.**
Note: Additional activities not shown here may have equally high importance/maturity score gaps. The importance and maturity score gaps for all activities are provided in the appendix.

Gartner®

Report Roadmap

Introduction	Gartner Score Overview and Model
Executive Summary	Key Findings
Path to Maturity	Next Steps on the Path to Increased Maturity
Next Steps	How Can Gartner Help
Appendix	Additional Pathways, Detailed Data, and Methodology

Gartner®

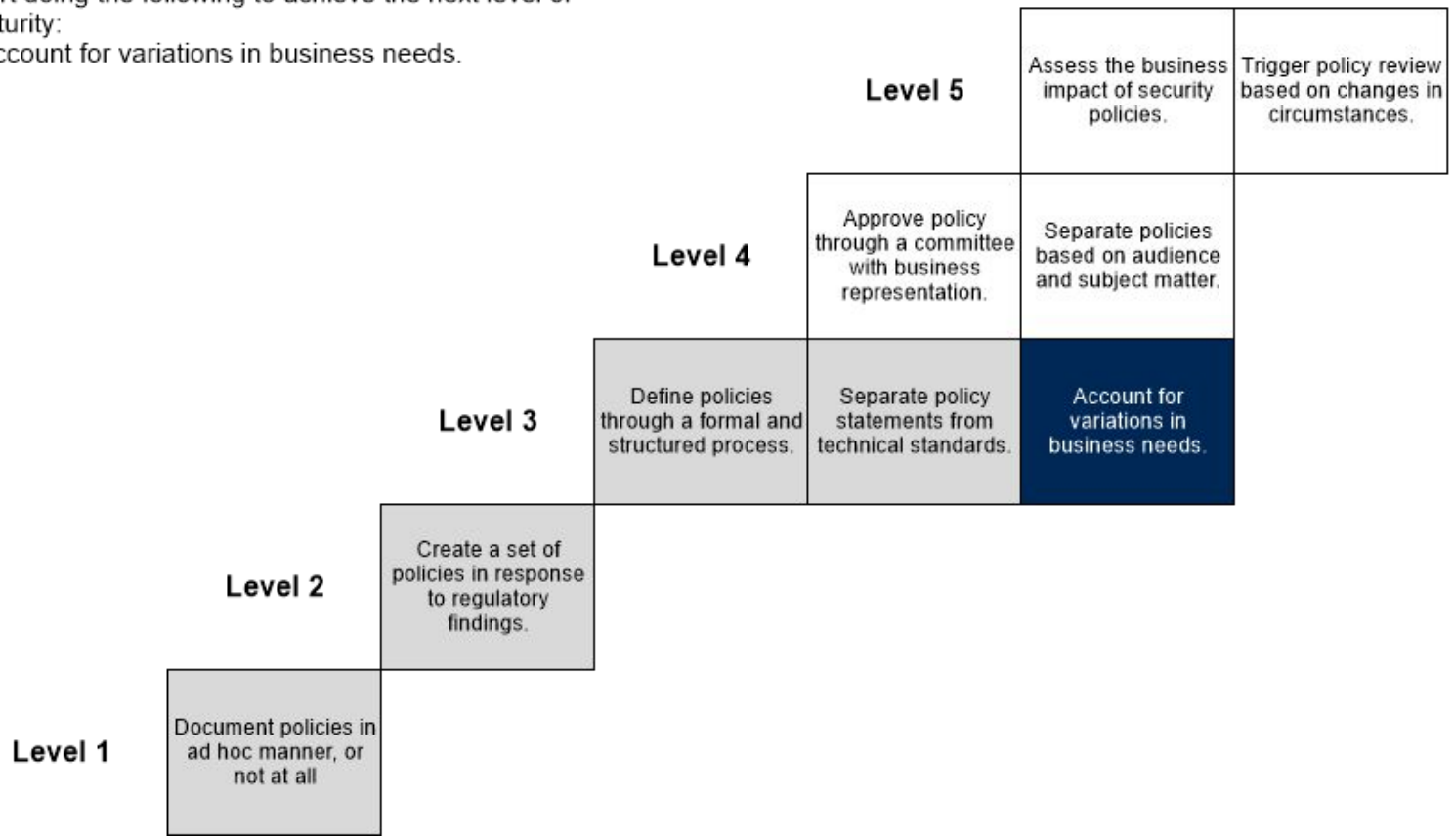
High Priority Area: Manage Policy

How the SRM function structures and documents a policy program to ensure business requirements are met

Path to Maturity

Start doing the following to achieve the next level of maturity:

• Account for variations in business needs.



Gartner®

Manage Policy

Featured Resources

Information Security Policy Library
Download and use security policies based on peer practice.

Foundational Practices

Ignition Guide to Drafting Information Risk Appetite Statements
Align policies with a commonly understood risk appetite statement to ensure risk mitigation efforts are in the company's best interests.

Progressive Practices

IDEXX's Power User-Led Policy Development
Incorporate feedback from power users within the company in order to tune and update policies in line with how work is changing.

Usable Policy for Decision Makers (SRI International)
SRI's security and risk management leaders rethink information security policies as a tool to enable independent, informed risk decision making across the enterprise. To achieve this, SRI collects and implements real-time user feedback to make policies, standards and guidelines more usable.

Note: Some documents may not be available as part of your current Gartner subscription.

Gartner®

Report Roadmap

Introduction	Gartner Score Overview and Model
Executive Summary	Key Findings
Path to Maturity	Next Steps on the Path to Increased Maturity
Next Steps	How Can Gartner Help
Appendix	Additional Pathways, Detailed Data, and Methodology

Gartner®

How Can Gartner Help Us?

Gartner Resources and Membership Support

Reach out to your client partner to:

- Discuss general support and design a long-term service plan based on your priorities for improvement.
- Schedule a conversation with a member of the Gartner team to identify specific strategies and resources to address maturity gaps.

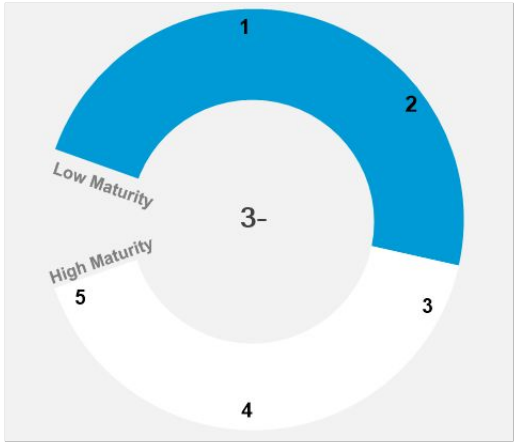
Contact the Member Support Center to set up a discussion with your Client Partner.

+1-866-913-6447 (US and International)

Available Monday-Friday, 7 AM - 7 PM Eastern Time

Key Takeaways to review with Gartner

Overall Maturity:



High priority activities based on importance and maturity level:

- Manage Policy
- Support Audit
- Measure Performance and more activities

Gartner®

Report Roadmap

Introduction	Gartner Score Overview and Model
Executive Summary	Key Findings
Path to Maturity	Next Steps on the Path to Increased Maturity
Next Steps	How Can Gartner Help
Appendix	Additional Pathways, Detailed Data, and Methodology

Gartner®

Maturity Level Definitions

Engage and Support Stakeholders

Interact With CEO and Board				
Level 1	**Level 2**	**Level 3**	**Level 4**	**Level 5**
The interaction between SRM and the board/CEO is very minimal and is only highlighted in the context of an overall IT report.	SRM provides ad hoc reporting through IT leadership only when incidents raise the concern of senior executives across the enterprise.	SRM develops and communicates standardized messaging on security and risk that get reported to the board and/or CEO periodically by the CISO.	SRM develops and communicates standardized reports in business-friendly language, aligned to business objectives that are made available to the board and CEO on a regular basis.	SRM enables the CEO and board to clearly understand and act on risks through formalized scheduled and proactive reporting, content customized to their needs with clear calls to action and guidance on how to interpret reports.
Foster Collaborative Risk Relationships				
Level 1	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Cross-functional risk relationships are reactive (based on incoming requests) and informal.	SRM conducts some strategic discussions with other risk management functions on major initiatives.	SRM defines and regularly updates roles and responsibilities for risk management functions and activities that impact multiple stakeholder functions.	SRM works with other stakeholders on future challenges and encourages staff across functions to minimize activity duplications and maximize collaboration.	SRM formally documents any and all activities requiring cross-functional input and establishes timelines, protocols and accountability for collaborative processes and information sharing across all stakeholders.
Enable Business Decisions				
Level 1	**Level 2**	**Level 3**	**Level 4**	**Level 5**
The SRM function does not contribute to or get involved in the overall business decision-making process.	The SRM function is invited to contribute to a small subset of business decisions on an ad hoc basis and/or is usually only involved after the business decision has been made.	The SRM function has a clear support role in helping stakeholders evaluate and make business decisions that have security implications.	The SRM function formally enables stakeholders to drive business decisions that have security implications based on some measurable impact.	The SRM function helps identify business opportunities and drive decisions that contribute to business success measured through a set of formalized metrics.
Drive Ownership and Accountability				
Level 1	**Level 2**	**Level 3**	**Level 4**	**Level 5**
The SRM function takes on accountability and ownership for risk decisions and rarely involves the business stakeholders.	The SRM function consults business stakeholders on an ad hoc basis and prioritizes responses to the business based on frequency of requests.	The SRM function identifies appropriate business stakeholders and proactively communicates business impacts and risk trade-offs to enable effective risk decisions.	The SRM function always identifies and limits decision making to true owners of risks in the business without imposing security's view of the "correct" decision.	The SRM function educates stakeholders on their roles and responsibilities and acts as the trusted advisor and facilitator of business-owned risk decisions.

Gartner®

Team Consensus

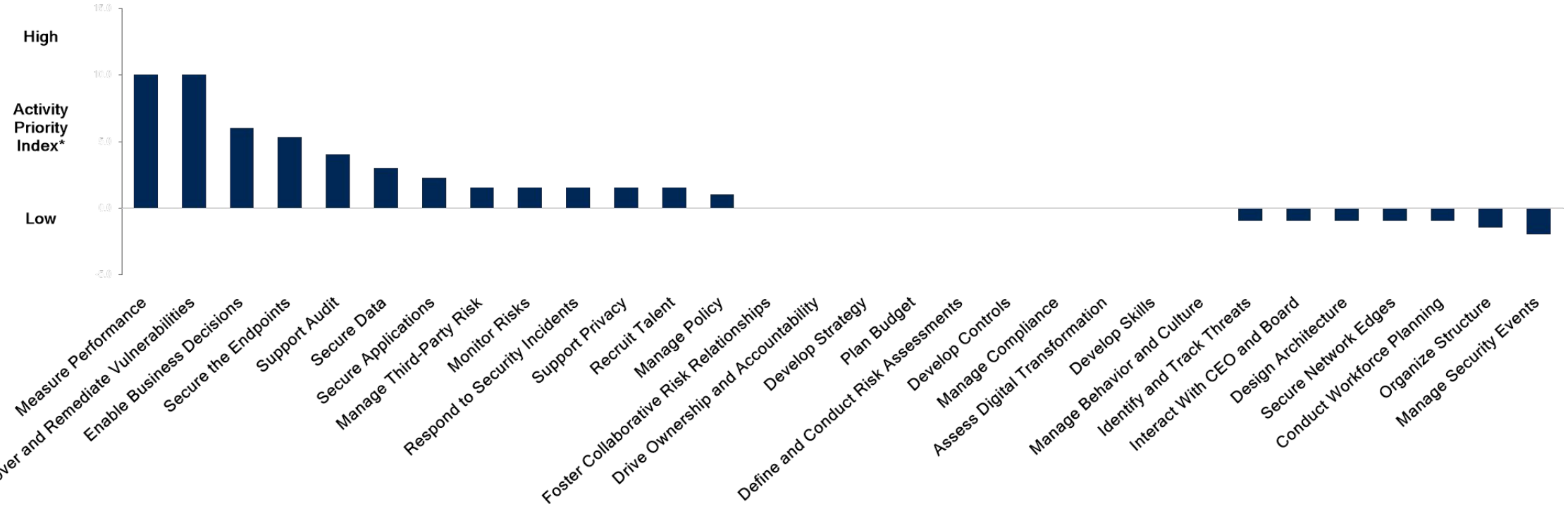
Maturity (Activities Ranked by Maturity Gap)

Objective	Activity	Benchmark	Overall (n = 2)	Leader Score (n = 1)	Staff Score (n = 1)	Gap (Leader minus Staff)
Deliver Assurance	Support Audit	Not Available	2.33	3.00	2.33	0.67
Manage the Function	Organize Structure	Not Available	3.00	3.50	3.00	0.50
Engage and Support Stakeholders	Drive Ownership and Accountability	Not Available	2.50	3.00	2.50	0.50
Manage the Function	Plan Budget	Not Available	2.50	3.00	2.50	0.50
Protect the Infrastructure	Secure Network Edges	Not Available	2.00	2.50	2.00	0.50
Manage Operations	Identify and Track Threats	Not Available	3.33	3.33	3.33	0.00
Engage and Support Stakeholders	Foster Collaborative Risk Relationships	Not Available	3.00	3.00	3.00	0.00
Manage the Function	Develop Strategy	Not Available	3.00	3.00	3.00	0.00
Manage the Function	Measure Performance	Not Available	3.00	3.00	3.00	0.00
Assess and Manage Risk	Define and Conduct Risk Assessments	Not Available	3.00	3.00	3.00	0.00
Manage Operations	Discover and Remediate Vulnerabilities	Not Available	3.00	3.00	3.00	0.00
Manage Operations	Manage Security Events	Not Available	3.00	3.00	3.00	0.00
Deliver Assurance	Manage Compliance	Not Available	3.00	3.00	3.00	0.00
Deliver Assurance	Assess Digital Transformation	Not Available	3.00	3.00	3.00	0.00
Manage People and Workforce Strategy	Develop Skills	Not Available	3.00	3.00	3.00	0.00
Manage People and Workforce Strategy	Manage Behavior and Culture	Not Available	3.00	3.00	3.00	0.00
Manage the Function	Manage Policy	Not Available	2.67	2.67	2.67	0.00
Protect the Infrastructure	Secure the Endpoints	Not Available	2.67	2.67	2.67	0.00
Engage and Support Stakeholders	Interact With CEO and Board	Not Available	2.50	2.50	2.50	0.00
Engage and Support Stakeholders	Enable Business Decisions	Not Available	2.50	2.50	2.50	0.00
Assess and Manage Risk	Manage Third-Party Risk	Not Available	2.50	2.50	2.50	0.00
Assess and Manage Risk	Monitor Risks	Not Available	2.50	2.50	2.50	0.00
Manage Operations	Respond to Security Incidents	Not Available	2.50	2.50	2.50	0.00
Manage People and Workforce Strategy	Recruit Talent	Not Available	2.50	2.50	2.50	0.00
Manage the Function	Design Architecture	Not Available	2.50	2.50	3.00	-0.50

Gartner®

What are the High Priority Areas for Your Function? (Leader Scores Only)

The Activity Priority Index identifies where the function is less mature in activities of greater importance.



n = 1

Highest Priority

- Measure Performance
- Discover and Remediate Vulnerabilities
- Enable Business Decisions

Lowest Priority

- Manage Security Events
- Organize Structure
- Conduct Workforce Planning and more activities

* Activity Priority Index: Activity Priority Index (API) for an activity is computed as average importance minus maturity multiplied by its average importance. A higher Activity Priority Index score indicates a greater priority to the organization.

Gartner®

Methodology Details

Survey Instrument

The diagnostic assesses functional activities along two primary dimensions: maturity and importance.

To assess maturity, respondents are presented a series of statements that represent component sub-activities of a particular functional activity. Respondents are asked to check all statements that represent currently performed sub-activities. Through an understanding of which sub-activities are currently being performed, Gartner can determine the level of maturity for any given functional activity.

Each whole level in the model is assigned one point. Gartner's proprietary logic calculates the fractional contribution of each sub-activity statement to the overall maturity score for that activity.

Scoring of Maturity

Range	Maturity Level
1.00–1.32	1
1.33–1.66	1+
1.67–1.99	2-
2.00–2.32	2
2.33–2.66	2+
2.67–2.99	3-
3.00–3.32	3
3.33–3.66	3+
3.67–3.99	4-
4.00–4.32	4
4.33–4.66	4+
4.67–4.99	5-
5	5

Setting Priorities (API Calculation)

To understand priorities, Gartner calculates the Activity Priority Index, which is weighted by importance.

The Activity Priority Index is calculated as follows:
API = (Importance – Maturity) x Importance

For precision, the maturity score expressed as a decimal is used in this calculation.

Higher API scores indicate very important or most important functional activities with low maturity, while lower API scores indicate lower importance activities with high maturity.

The API proposes a set of priorities on the assumption that highly important activities with low maturity should be targeted first to increase functional performance.

Gartner®

Calculation of Maturity Scores

Introduction

Gartner Score takes a unique approach to assessing maturity. It disaggregates the five-level maturity model for a given activity into 5–15 discrete statements that describe sub-activities. Those sub-activities are each associated with a maturity level, one to five, of the given activity.

The entire five-level maturity model for an activity is assigned five points, one point for each level. Within a level, the one point is allocated evenly across all of the sub-activities associated with that level. If there is one sub-activity, it is allocated 1.0 point; if there are two, each is worth 0.5 points, if there are three, then 0.33 points each, and so forth. Note that the sum of the fractional points across all the sub-activities for each level is 1.0 and the sum across all levels of an activity is always 5.0.

Assessing Maturity

Each sub-activity is then directly assessed by respondents as being present and effective in the organization, or not.

Rather than creating a maturity score for each respondent for an activity and then averaging those, Gartner first aggregates the responses across all respondents for each sub-activity. To be scored as a “Yes” (present and effective) for the organization, more than 50% of the respondents must have assessed that Sub-Activity as a “Yes”. Otherwise that sub-activity is scored as a “No” overall. In the case of a single respondent (only one surveyed, or sub-group of one) the individual response is taken as the “group” response.

This approach offers two important advantages. First, it provides a better assessment of maturity, as each individual sub-activity must be judged by a majority of respondents to be present and effective to contribute to the overall maturity score for an activity. Second, it allows for more precise identification of which components of that level of maturity are already present and which specific next steps the organization should take to achieve a particular higher level of maturity for a given activity.

Calculating Maturity Scores

Sub-activities scored as a “Yes” for the organization earn the full fractional point value associated with them (as described in the second paragraph on this page). Those scored as “No” receive zero points.*

The earned fractional values of the sub-activities are then totaled to calculate the organization’s maturity score for that activity. Scores ranging from x.00 to x.32 are assigned an ordinal value of x (e.g., 3.15 is presented as “3”). Those ranging from x.33 to x.66 are reported as x+ (e.g., 3.50 is presented as “3+”), and those from x.67 to x.99 as (x+1)- (e.g., 3.83 is presented as “4-”).

Please see the next page for an example.

* An exception occurs when a function is generally operating at a higher level of maturity for an activity but still performing a lower-level sub-activity that should be discontinued. In this situation, the overall maturity score is penalized by subtracting one-half of the assigned fractional value of that sub-activity.

Gartner®

Calculation of Maturity Scores

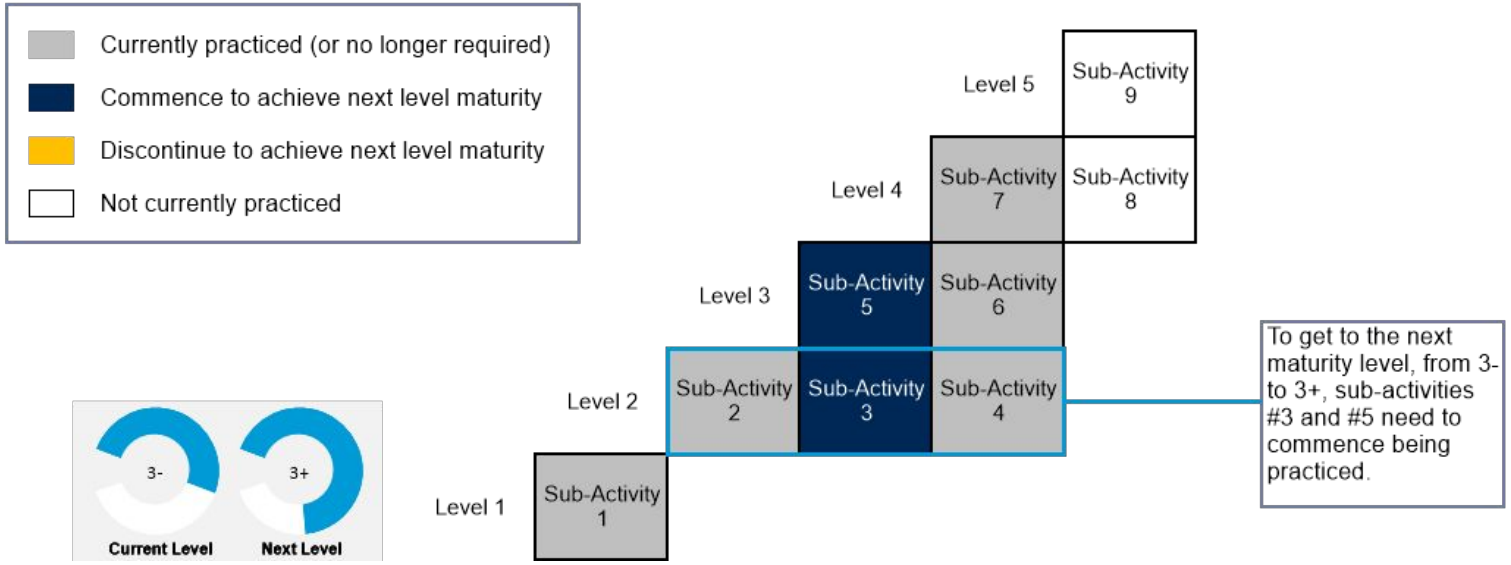
Individual Survey Respondent Answers

In this example, there are 3 sub-activities at Level 2, each worth 0.33 points.

Activity A	Maturity Level	Assigned Points	Resp. 1	Resp. 2	Resp. 3	Resp. 4	Resp. 5	Resp. 6	% Yes	Group Resp.	Earned Points
Sub-activity 1	1	1.00	Y	Y	Y	Y	Y	Y	100%	Y	1.00
Sub-activity 2	2	0.33	Y	Y	Y	N	Y	N	67%	Y	0.33
Sub-activity 3	2	0.33	Y	N	Y	N	Y	N	50%	N	0.00
Sub-activity 4	2	0.33	Y	N	Y	Y	Y	N	67%	Y	0.33
Sub-activity 5	3	0.50	Y	N	Y	Y	N	N	50%	N	0.00
Sub-activity 6	3	0.50	Y	N	N	Y	Y	Y	67%	Y	0.50
Sub-activity 7	4	0.50	Y	N	Y	Y	Y	N	67%	Y	0.50
Sub-activity 8	4	0.50	N	N	Y	N	N	N	17%	N	0.00
Sub-activity 9	5	1.00	N	N	N	N	N	N	0%	N	0.00
Total		5.00									2.66
										Maturity Score	2+

Group responses to sub-activities are calculated, and then points are awarded. Here, only two of three sub-activities (#2 and #4) at maturity level 2 were assessed as "present" and "effective" by more than 50% of the respondents, leading to an award of 0.66 of the entire 1.0 points available at Level 2.

Path to Maturity for Activity A



To get to the next maturity level, from 3- to 3+, sub-activities #3 and #5 need to commence being practiced.

Gartner