Annex 1

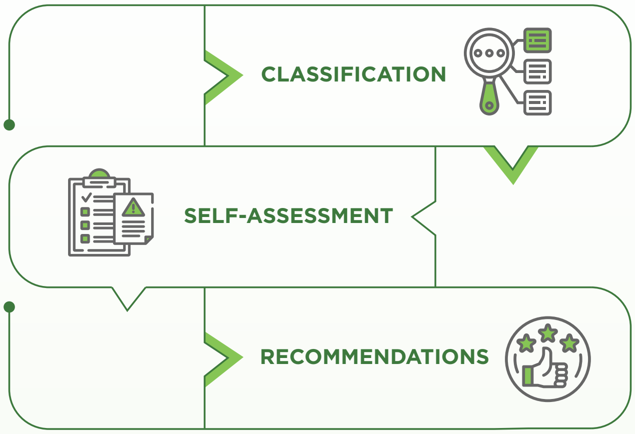
Description of the self-assessment tool for the healthcare sector provided by the IDB

The self-assessment tool for the healthcare sector is designed to help heads of organizations evaluate their cybersecurity status based on industry best practice.

Since this is a self-assessment tool, it involves no interaction with a consultant or specialist who can complement and contextualize the questions to help users understand them based on their knowledge. One of the main challenges in developing the tool was to generate self-contained questions that are easy to understand.

Figure 1 shows the tool's three-stage logic: **classification, self-assessment, and recommendations.**

FIGURE 1 • Implemented logic



The aim of the classification stage is to define a target cybersecurity level for the organization. The tool establishes three potential organizational levels (BASIC, INTERMEDIATE, and ADVANCED) on which the information security requirements are based. This classification determines which questions are included in the self-assessment.

Given the wide array of healthcare sector companies and organizations that will be using the self-assessment tool, it is first important to understand the type of organization being assessed. **The types of organizations covered by version v0.7.2 are:**

- Hospitals
- Pharmacies
- Laboratories
- Ministry or regulatory bodies
- Healthcare providers or provider groups or others

The tool offers a set of questions for each type of organization to gauge its size according to different business variables. The questions were designed based on the organizational factors HITRUST uses to define the implementation levels.

Table 1 shows the classification questions used in version v0.7.2 of the self-assessment tool, listing the source used to design them, or no source if the question was created based on the team's experience.

TABLE 1 • Ranking questions used in version 0.7.2

Question and answer	Source
How many beds does the organization have? • BASIC: Fewer than 200 • INTERMEDIATE: Between 200 and 750 • ADVANCED: More than 750	HITRUST
How many patients do you admit per year? • BASIC: Fewer than 7,500 • INTERMEDIATE; Between 7,500 and 20,000 • ADVANCED: More than 20,000	HITRUST
How many people are eligible to receive care at the organization (members/other)? • BASIC: Fewer than 1,000,000 • INTERMEDIATE; Between 1,000,000 and 7,500,000 • ADVANCED: More than 7,500,000	HITRUST
How many medical consultations are offered per year? • BASIC: Fewer than 1,000,000 • INTERMEDIATE; Between 1,000,000 and 6,000,000 • ADVANCED: More than 6,000,000	HITRUST
How many medical service providers (labs/imaging/other) do you have? • BASIC: Fewer than 10 • INTERMEDIATE; Between 10 and 30 • ADVANCED: More than 30	(no source)
How many medical studies are performed each year? • BASIC: Fewer than 25,000 • INTERMEDIATE; Between 25,000 and 100,000 • ADVANCED: More than 100,000	(no source)

The classification questions depend on the type of organization. If the answers yield a mix of different levels, the tool suggest using the higher of the levels. For example, if a hospital answers that it has more than 750 beds (ADVANCED) and admits between 7,500 and 20,000 patients per year (INTERMEDIATE), the tool will suggest answering the self-assessment questionnaire at the ADVANCED level. This classification is simply a recommendation and the user can change it because there may be other factors not covered by the tool (e.g., regulatory) that place the organization on another level.

The next step is to use a set of questions to evaluate the organization's current level of cybersecurity based on the NIST-CSF. The questions for this evaluation are broken down by organizational level (BASIC, INTERMEDIATE, and ADVANCED).

Table 2 shows the number of questions for each NIST-CSF function and organizational level at which the self-assessment tool is implemented.

This model produced a limited number of questions that increase at each level. The total number of questions for a basic level evaluation is 25, increasing to 44 (25+19) for the intermediate level and 66 (25+19+22) for the advanced level.

For more details on the tool's evaluation questions and the logical connections between them, we recommend reading the Annex **"Self-assessment questions for the health sector provided by the IDB."**

Once an organization completes the self-assessment tool, the next step is the recommendation stage. At this stage, the tool calculates a score for each NIST-CSF function and category by averaging the results for each function and category. Each option for each question has a fixed value assigned to it.

Figure 2 shows the score for each NIST-CSF function in the form of a radar chart (in version v0.7.2 of the tool, with a fictitious example).

The recommendations consist of a general description and specific actions to be implemented to improve the organization's maturity level in each NIST-CSF category. The tool selects which recommendations to display based on the score obtained in each category and an acceptance threshold that has been pre-established by experts.

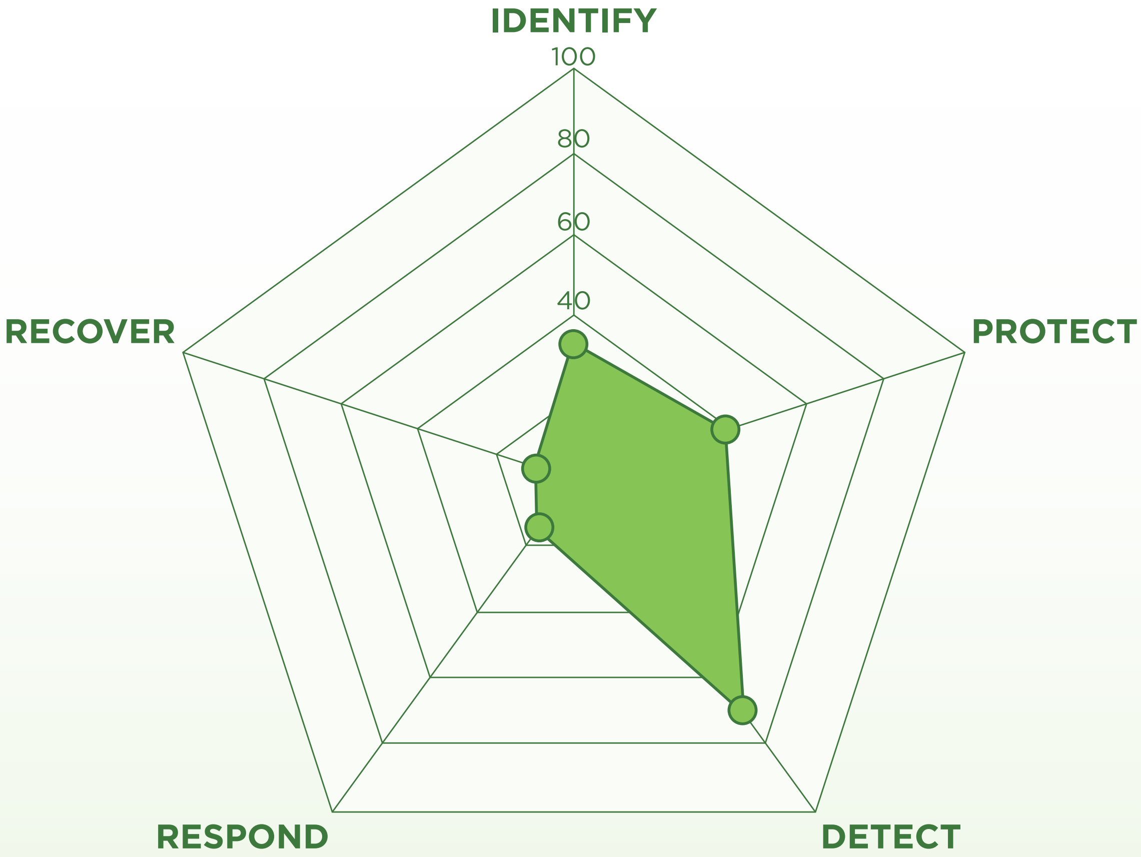
Two activities were carried out to ensure the tool does what it is supposed to. The first was a focus group with representatives from different universities in the region. The second was a proof of concept of the tool at LAC health organizations with the aim of validating how it works in the field. **Both activities yielded lessons and recommendations, some of which were included in the current version, and the team created a list of potential future improvements, including:**

- weighted scoring,
- improvements to the rules for suggesting recommendations or including/excluding concrete actions in the recommendations,
- adding material to the questions to support skill development or make the questions more understandable,
- having a more accurate profile of the person filling out the self-assessment in order to personalize the questions.

TABLE 2 • Questions grouped by NIST-CSF function

	Basic	Intermediate	Advanced
GENERAL	5	0	0
IDENTIFY	3	8	9
PROTECT	11	5	5
DETECT	3	2	4
RESPOND	2	2	2
RECOVER	1	2	2
TOTAL	**25**	**19**	**22**

FIGURE 2 • Results from an INTERMEDIATE level self-assessment



Annex 2

Self-assessment questions for the healthcare sector provided by the IDB

This annex describes the questions used by the self-assessment tool for the healthcare sector described in the previous annex.

The questions were based on each NIST-CSF subcategory, though there is not a one-to-one correlation between subcategories and questions. Some questions are used to assess more than one subcategory. Because the recommendations were based on the NIST-CSF categories, it was important to ensure there was at least one question associated with each category.

Table 3 shows the questions included in version v0.7.2 of the self-assessment tool.

TABLE 3 • Questions included in the v0.7.2 version of the self-assessment tool

Identifier	Purpose	Category	Question
GR-SC1	General	-	Do you have a team dedicated to information security? Options: • No • Yes
GR-SC2	General	-	What size is the current information security team, as compared to the number of people working at the organization? Options: • 1 for every 1,000 • 1 for every 100 • 1 for every 10 • 1 for every 5

TABLE 3 • Questions included in the v0.7.2 version of the self-assessment tool (*cont.*)

Identifier	Purpose	Category	Question
GR-SC3	General	-	Do you allot a portion of the budget to cybersecurity? Options: • No • Yes
GR-SC4	General	-	What percentage of the IT budget goes to cybersecurity? (thresholds) If the IT and cybersecurity budgets are separate, the answer should be expressed as a percentage of the combined budgets. Options: • Under 1% • Between 1% and 3% • Between 3% and 6% • Over 6%
GR-SC5	General	-	What size is the current IT team, as compared to the number of people working at the organization? Options: • 1 for every 1,000 • 1 for every 100 • 1 for every 10 • 1 for every 5
ID-B1	Identify	ID.AM	DO YOU HAVE AN UP-TO-DATE inventory for any of the following assets? • Physical devices (PCs, mobile devices, routers, servers, storage, etc.). • Software applications, systems, and platforms

TABLE 3 • Questions included in the v0.7.2 version of the self-assessment tool (*cont.*)

Identifier	Purpose	Category	Question
ID-B1	Identify	ID.AM	• Networks Options: • None • YES, I have inventoried some of the organization’s assets, but the individually detailed information is not up to date. • YES, I have inventoried all of the organization’s assets, but the individually detailed information is not up to date. • YES, I have inventoried all of my organization’s assets, and the individually detailed information is up to date.
ID-B2	Identify	ID.AM	Who handles issues related to information security or cybersecurity at your organization? Options: • No one • The IT team • The dedicated security staff within IT • The dedicated security team independent from IT

TABLE 3 • Questions included in the v0.7.2 version of the self-assessment tool (*cont.*)

Identifier	Purpose	Category	Question
ID-B3	Identification	ID.GV	Do you have to comply with any industry-specific regulations such as the Personal Data Protection Act or the Medical Records Act? Options: • No • Yes
ID-M1	Identification	ID.AM	Is the information related to the assets classified according to applicable laws, policies, standards, and guidelines? An example of classification is categorizing the information as public, for internal use, confidential, or secret. Options: • No • Partially • Yes
ID-M2	Identify	ID.AM	Does your organization have procedures in place to ensure protection of the flow of internal and external information? Options: • No • Partially • Yes

TABLE 3 • Questions included in the v0.7.2 version of the self-assessment tool (*cont.*)

Identifier	Purpose	Category	Question
ID-M3	Identification	ID.AM	Have the following roles been assigned? • Chief Information Security Officer (CISO) • Security Incident Response Team • Security risk manager • Vulnerability manager Options: • None • CISO • All of them
ID-M4	Identification	ID.GV	Which of the following elements are used at your organization? • Information security policies • Information security processes • Information security procedures Options: • None • Only procedures • Only processes and procedures • All of them

TABLE 3 • Questions included in the v0.7.2 version of the self-assessment tool (*cont.*)

Identifier	Purpose	Category	Question
ID-M5	Identify	ID.GV	Do you have the support of a multidisciplinary team (lawyers and technicians) to analyze the requirements of the applicable regulations? Options: • No • Yes
ID-M6	Identification	ID.RA	Are the assets' vulnerabilities identified and analyzed? Options: • No • No, but corrective actions are taken when notified. • Yes, for critical assets. • Yes, and there is an associated process for managing vulnerabilities.
ID-M7	Identification	ID.RA	Are risk and impact assessments based on threats and vulnerabilities? Options: • No • Yes • Yes, and they serve as the basis for defining the controls necessary to bring the risk to an acceptable level for the organization.

TABLE 3 • Questions included in the v0.7.2 version of the self-assessment tool (*cont.*)

Identifier	Purpose	Category	Question
ID-M8	Identification	ID.SC	Do you have service level agreements with critical service providers? Options: • No • Yes
ID-A1	Identification	ID.AM	Have you defined policies and procedures that set the standards for asset inventorying? Options: • No • Yes
ID-A2	Identification	ID.AM	Do you have automatic tools for asset inventory management? Options: • No • Some • Yes
ID-A3	Identification	ID.AM	Is the inventory updated as soon as it changes? Options: • No • Yes
ID-A4	Identify	ID.BE	Have you identified the suppliers, systems, and overall resources (internal and external) needed to deliver your organization’s critical services? Options: • No • Partially • Yes

TABLE 3 • Questions included in the v0.7.2 version of the self-assessment tool (*cont.*)

Identifier	Purpose	Category	Question
ID-A5	Identify	ID.GV	Do you have an ISMS in place with continuous improvement procedures? Options: • No • In process of implementation • Yes
ID-A6	Identify	ID.GV	Is there an information security committee? Options: • No • Yes
ID-A7	Identify	ID.GV	Does the information security committee have legal counsel to ensure compliance with current regulations? Options: • No • Yes
ID-A8	Identify	ID.RM	Do you have a formal risk treatment plan? Options: • No • Yes
ID-A9	Identify	ID.SC	Do your suppliers and external partners perform a supply chain risk assessment? Options: • No • Yes

TABLE 3 • Questions included in the v0.7.2 version of the self-assessment tool (*cont.*)

Identifier	Purpose	Category	Question
PR-B1	Protect	PR.AC	Do you have a team in charge of user management (identities and credentials)? Options: • I do not have identified users. • YES, and it is done on a best-effort basis. • YES, and it is systematized with a formal process. • YES, and it is systematized with a formal process and audited periodically.
PR-B2	Protect	PR.AC	Do you have a team in charge of authorization management for devices? Options: • I do not have identified devices. • YES, and it is done on a best-effort basis. • YES, and it is systematized with a formal process. • YES, and it is systematized with a formal process and audited periodically.
PR-B3	Protect	PR.AC	Do you implement physical access controls? Options: • No • For servers only. • Servers and other equipment are locked up or under video surveillance.

TABLE 3 • Questions included in the v0.7.2 version of the self-assessment tool (*cont.*)

Identifier	Purpose	Category	Question
PR-B4	Protect	PR.AC	Does your organization have remote accesses? Options: • No • Yes
PR-B5	Protect	PR.AC	Do you implement remote access controls? Options: • No • With multiple tools, without centralized management (e.g. RDP, VNC, etc.), and without extra security measures. • With centralized management, using tools such as VPN + RDP, VPN + VNC, among others. • With centralized management and properly implemented through processes.
PR-B6	Protect	PR.DS	Is stored data (on paper, disks, tapes, backups, etc.) protected by adding controls such as physical access control, logical access control, encryption, etc.? Options: • No • Only in some cases. • Yes • YES and the encryption measures are validated as adequate for the information's confidentiality level.

TABLE 3 • Questions included in the v0.7.2 version of the self-assessment tool (*cont.*)

Identifier	Purpose	Category	Question
PR-B7	Protect	PR.DS	Is data in transit protected using technologies such as SSL, HTTPs, VPNs, etc.? Options: • No • YES, when in transit to outside the organization. • YES, when in transit inside and outside the organization. • YES, in both directions, and the encryption measures are validated as adequate for the information's confidentiality level.
PR-B8	Protect	PR.DS	In the event that your employees or suppliers handle confidential information, do you have signed confidentiality agreements? Options: • No • Only with suppliers, not with employees. • With employees and some suppliers. • With employees and all suppliers.
PR-B9	Protect	PR.IP	Is the information backed up? Options: • No • YES, locally • YES, remotely

TABLE 3 • Questions included in the v0.7.2 version of the self-assessment tool (*cont.*)

Identifier	Purpose	Category	Question
PR-B10	Protect	PR.IP	Are backups tested? Options: • No • Yes • YES, frequently
PR-B11	Protect	PR.PT	Are log records of assets (applications, operating systems, network equipment, etc.) available? Options: • No • YES, but no retention policies are in place. • YES, and retention policies are in place. • YES, retention policies are in place and periodically reviewed.
PR-M1	Protect	PR.AC	Does it separate environments for each person to access only the information relevant to him/her? Options: • No • There is separation of environments, but all users/roles can access any of them. • Yes

TABLE 3 • Questions included in the v0.7.2 version of the self-assessment tool (*cont.*)

Identifier	Purpose	Category	Question
PR-M2	Protect	PR.AC	Is your network segmented according to asset sensitivity and exposure? Options: • No • YES, my network is segmented but there are no clear criteria for segmentation (risks, information sensitivity, etc.). • Yes
PR-M3	Protect	PR.AT	Do you have an information security awareness and training program? Options: • No • Talks on the subject are offered occasionally. • The personnel periodically receive talks on the subject. • Yes
PR-M4	Protect	PR.DS	Do you calculate the projected growth of the systems that support the services? Options: • No • A growth prediction for the lifespan of the equipment is made at the time of purchase. • Yes

TABLE 3 • Questions included in the v0.7.2 version of the self-assessment tool (*cont.*)

Identifier	Purpose	Category	Question
PR-M5	Protect	PR.IP	Do you have a defined baseline for the information systems' configuration? Options: • No • YES, but it is not reviewed unless there are changes to the system. • YES, and it is reviewed periodically. • YES, it is reviewed periodically and configuration management processes are followed.
PR-A1	Protect	PR.AT	Do you have a specialized information security awareness and training program for privileged users? Options: • No • Talks on best practices are offered occasionally. • The personnel receive regular talks on best practices. • YES, and a training plan on information security or cybersecurity is followed.
PR-A2	Protect	PR.IP	Do you implement the systems development life cycle? Options: • No • Yes • Yes, and it is formally documented.

TABLE 3 • Questions included in the v0.7.2 version of the self-assessment tool (*cont.*)

Identifier	Purpose	Category	Question
PR-A3	Protect	PR.IP	Does your systems development life cycle have embedded safety tasks (S-SLDC)? Options: • No • YES, some activities are embedded but not systematically. • YES, activities are included and performed in continuous improvement mode.
PR-A4	Protect	PR.MA	Do you plan the management and repair of your assets? Options: • No • Yes, but I have no record of those repairs. • Yes, and they are recorded. • Yes, and there is a process for approving repairs.
PR-A5	Protect	PR.PT	Do you have standardized and centralized asset log records? Options: • No • YES, they are centralized. • YES, they are centralized and standardized for use.

TABLE 3 • Questions included in the v0.7.2 version of the self-assessment tool (*cont.*)

Identifier	Purpose	Category	Question
DE-B1	Detect	DE.CM	Do you have an antivirus solution? Options: • No • On some devices • On all devices
DE-B2	Detect	DE.CM	Is the antivirus solution up to date? Options: • No • Yes
DE-B3	Detect	DE.CM	Are the alerts from your antivirus solution checked? Options: • No • YES, occasionally • YES, there is an associated process.
DE-M1	Detect	DE.CM	Is the network monitored for potential cybersecurity events? Options: • No • YES, I have events configured in the organization's existing assets (e.g. firewalls). • YES, I have specific rules implemented in the organization's security monitoring systems.

TABLE 3 • Questions included in the v0.7.2 version of the self-assessment tool (*cont.*)

Identifier	Purpose	Category	Question
DE-M2	Detect	DE.CM	How often are vulnerability scans performed? Options: • NO scans are performed. • YES, the main systems are scanned as an isolated effort. • YES, all assets of the organization which have access to sensitive information are scanned as an isolated effort • YES, periodically, and they are subjected to vulnerability management as well.
DE-A1	Detect	DE.AE	Do you have knowledge of the normal behavior of your systems and expected data flows? For example, the number of users that normally use a system, the regular network data flow, the number of log records a system writes, or the number of emails sent per day in the organization, among others. Options: • No • YES, for the main systems. • YES, with defined thresholds and cause/impact analysis when thresholds are exceeded.

TABLE 3 • Questions included in the v0.7.2 version of the self-assessment tool (*cont.*)

Identifier	Purpose	Category	Question
DE-A2	Detect	DE.AE	Is event data aggregated and correlated from multiple sources and sensors? Options: • No • YES, on an ad-hoc basis • YES, using a security information and event management (SIEM) system. • YES, and analyzed with a security operations center (SOC).
DE-A3	Detect	DE.CM	Is the activity of external service providers monitored for potential cybersecurity events? Options: • No • YES, attempts at activity not allowed in the defined access mechanisms (e.g. unanticipated activity on VPNs) are monitored.

TABLE 3 • Questions included in the v0.7.2 version of the self-assessment tool (*cont.*)

Identifier	Purpose	Category	Question
DE-A4	Detect	DE.DP	Do you have security event detection processes and procedures in place? A security event is an occurrence identified in the state of a system, service, or network that may be relevant to the security of the system, service or network. Options: • No • Yes • YES, and lessons learned from incidents are incorporated as incident improvement.
RS-B1	Respond	RS.RP	Do you have a defined way of dealing with an information security incident? Options: • No • YES, undocumented and without defined responsibilities. • YES, undocumented and with defined responsibilities. • YES, documented and with defined responsibilities.

TABLE 3 • **Questions included in the v0.7.2 version of the self-assessment tool (*cont.*)**

Identifier	Purpose	Category	Question
RS-B2	Respond	RS.CO	Are incidents communicated and coordinated with internal and external stakeholders, as appropriate? Options: • No • YES, with an in-house team. • YES, with in-house and external parties, where appropriate.
RS-M1	Respond	RS.MI	What type of actions do you take when facing an information security incident? Options: • None. • It is contained, for example by isolating the affected assets. • It is contained and measures are taken to reduce its impact.
RS-M2	Respond	RS.AN	Are the causes of an incident analyzed and is information collected as evidence? Options: • No • YES, the causes and impact of incidents are analyzed. • YES, the causes and impact of incidents are analyzed and a forensic analysis is performed, where appropriate.

TABLE 3 • Questions included in the v0.7.2 version of the self-assessment tool (*cont.*)

Identifier	Purpose	Category	Question
RS-A1	Respond	RS.IM	Are lessons learned during incident analysis incorporated for future response activities? Options: • No • Only in some cases. • YES, in all cases.
RS-A2	Respond	RS.CO	In the event of an incident, are those involved notified of the impact on the security of their data? Options: • No • Only on some occasions, although this may involve regulatory non-compliance. • YES, whenever I have a regulatory obligation. • YES, in all cases.

TABLE 3 • Questions included in the v0.7.2 version of the self-assessment tool (*cont.*)

Identifier	Purpose	Category	Question
RC-B1	Recover	RC.RP	Are recovery processes and procedures implemented and maintained to ensure timely restoration of affected systems or assets? Options: • I do NOT have recovery plans for my critical systems. • YES, I have recovery plans for some critical systems. • YES, I have recovery plans for all my critical systems, but I do not test them periodically. • YES, I have recovery plans for all my critical systems and test them periodically.
RC-M1	Recover	RC.RP	Are recovery processes and procedures documented and communicated? Options: • No • YES, they are documented but not communicated. • YES, they are documented and communicated.

TABLE 3 • Questions included in the v0.7.2 version of the self-assessment tool (*cont.*)

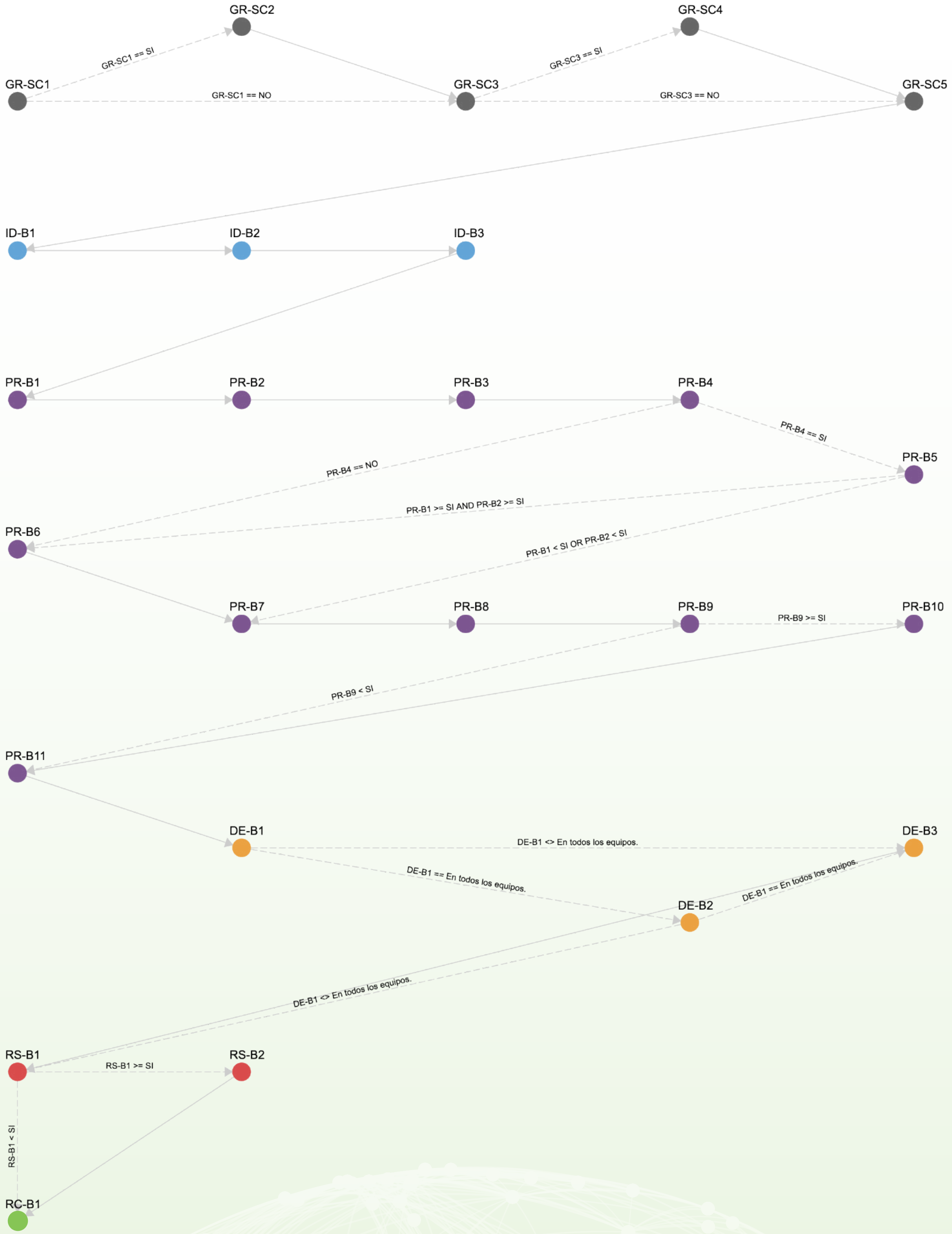
Identifier	Purpose	Category	Question
RC-M2	Recover	RC.IM	Are lessons learned during recovery incorporated for future activities? Options: • No • Only in some cases. • YES, in all cases.
RC-A1	Recover	RC.RP	Do you conduct drills to validate recovery processes and procedures? Options: • No • Yes
RC-A2	Recover	RC.CO	Are communications with stakeholders (internal and external) and public relations managed? Options: • No • Yes • YES and there is a plan for such management.

The questions may be interdependent, so a rules language was defined in the tool to determine the cases in which a certain question should or should not be asked. This functionality improves usability because the questions can expand on or are related to previous questions. For example, if someone answers that there is no remote access at their organization (question **PR-B4**), the question about what controls are implemented over that remote access does not apply (question **PR-B5**).

A dependency graph was created to visually represent the dependencies. The questions are shown in the form of a circle, the question identifier is shown above the circle, and the edges are the transitions between questions. The color of the circle matches the color of the NIST function associated with the question.

Figure 3 shows the graph of dependencies between the questions at the BASIC organizational level implemented in version v0.7.2 of the self-assessment tool.

FIGURE 3 • Degree of dependencies between questions at the BASIC organizational level implemented in version v0.7.2 of the self-assessment tool.



The conditions on the edges of the graph have logical AND and OR operators, while the expressions use comparison operators.

To make it easier to read the graph, comparison operators should be read as explained in the examples below.

Consider question DE-B1, which reads, "Do you have an antivirus solution?" Your choices are:

1. No
2. On some devices
3. On all devices

The options are presented in order, in the form of a list. So when we say PR-B9 = "On all computers," this means the index of the answer to PR-B9 is equal to 3. In this case, it is a condition that says whether you have antivirus software on all computers or not.

If we wanted to write a condition which represents that there is antivirus software but it does not matter on how many computers, it could be written in any of the following ways:

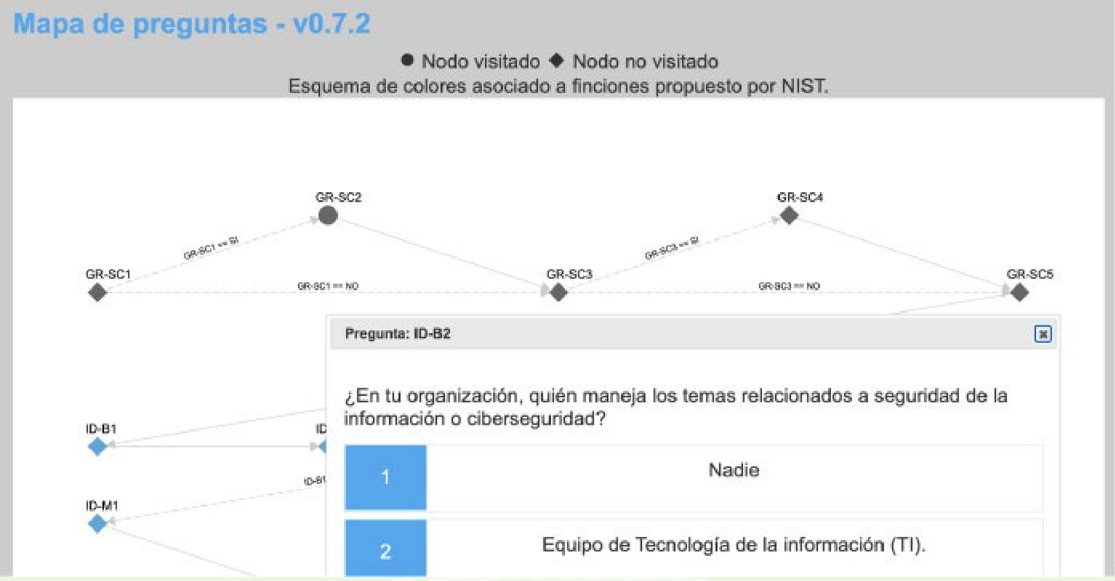
- PR-B9 <> "NO"
- PR-B9 >= "On some computers"

We compare the indices of the options, and therefore both expressions are equivalent.

To simplify the graphic, "YES" is shown instead of the full text when the text of the option starts with "YES".

While answering the questionnaire in the self-assessment tool, you can request to see the dependency graph. In this case, the graph is presented as filtered by the organizational level (BASIC, INTERMEDIATE, or ADVANCED) and the questions that have been answered are marked. The node is represented by a diamond shape. When you click on the node that represents the question on the dependency graph, a window pops up with the data for that question, as shown in Figure 4.

FIGURE 4 • Popup with the data of said question*



Mapa de preguntas - v0.7.2

● Nodo visitado ◆ Nodo no visitado
Esquema de colores asociado a finciones propuesto por NIST.

Pregunta: ID-B2

¿En tu organización, quién maneja los temas relacionados a seguridad de la información o ciberseguridad?

1 Nadie

2 Equipo de Tecnología de la información (TI).

* Currently the tool is only available in spanish, the english version is forthcoming.

TABLE 4 • Question dependencies

Identifier	Dependence
GR-SC2	ResponseIndex('GR-SC1') == 4
GR-SC4	ResponseIndex('GR-SC3') == 4
ID-M1	ResponseIndex('ID-B1') > 1
ID-M3	ResponseIndex('ID-B2') > 1
ID-M5	ResponseIndex('ID-B3') == 4
ID-M6	ResponseIndex('ID-B1') > 1
ID-A1	ResponseIndex('ID-B1') > 1
ID-A2	ResponseIndex('ID-B1') > 1
ID-A3	ResponseIndex('ID-B1') > 1
ID-A4	ResponseIndex('ID-B1') > 1
ID-A5	ResponseIndex('ID-M4') == 4
ID-A6	ResponseIndex('ID-M3') > 2
ID-A7	ResponseIndex('ID-A5') == 4
ID-A8	ResponseIndex('ID-M7') == 4
ID-A9	ResponseIndex('ID-M8') == 4
PR-B5	ResponseIndex('PR-B4') == 4
PR-B6	(ResponseIndex('PR-B1') > 1) && (ResponseIndex('PR-B2') > 1)
PR-B10	ResponseIndex('PR-B9') > 2
PR-A1	ResponseIndex('PR-M3') > 2
PR-A3	ResponseIndex('PR-A2') > 2
PR-A5	ResponseIndex('PR-B11') > 1
DE-B2	ResponseIndex('DE-B1') == 4
DE-B3	ResponseIndex('DE-B1') == 4
DE-A2	ResponseIndex('DE-M1') > 2
DE-A3	ResponseIndex('DE-M1') > 2
DE-A4	(ResponseIndex('DE-A1') > 2) && (ResponseIndex('DE-A2') > 1)
RS-B2	ResponseIndex('RS-B1') > 1
RS-M1	ResponseIndex('RS-B1') > 1
RS-M2	ResponseIndex('RS-B1') > 1
RS-A1	((ResponseIndex('RS-B1') > 2) && (ResponseIndex('RS-M2') > 2))
RS-A2	((ResponseIndex('RS-B1') > 1) && (ResponseIndex('RS-B2') > 1))
RC-M1	ResponseIndex('RC-B1') > 1
RC-M2	ResponseIndex('RC-B1') > 1
RC-A1	ResponseIndex('RC-B1') == 4
RC-A2	ResponseIndex('RC-B1') == 4

AUTHORS: Pablo Alzuri, Florencia Cabral, Santiago Paz, Ariel Nowersztern and Pablo Libedinsky.
DESIGN: www.souvenirme.com

The opinions expressed in this publication are those of the authors and do not necessarily reflect the views of the Inter-American Development Bank, its Board of Directors, or the countries they represent.