A mid-sized healthcare organization, 'SouthernCross', aims to strengthen its cybersecurity posture. Due to the sensitive nature of patient data and stringent regulatory requirements, SouthernCross needs a comprehensive, adaptable cybersecurity strategy. They decide to use the proposed cybersecurity capability maturity framework to assess and improve their current capabilities.

To make the case study less complex to understand, we are only considering **3 core domains** (Risk Management, Identity and Access Management, and Data Security) and **2 elective domains** (Network Security and Compliance & Legal) for SouthernCross. Ideally, all core domains would need to be considered, along with the elective domains chosen based on organizational needs. We'll walk through two practices per tier for each domain, illustrate how these practices are implemented, track metric achievement, and calculate the scores to derive the final maturity levels.

Within each selected domain, SouthernCross categorizes the practices based on the stratified structure provided by the framework. They opt for different target tiers for each domain:

- For **Risk Management (RM)**, **Identity and Access Management (IAM)**, and **Data Security (DS)**, SouthernCross aims for the **Intermediate Tier** due to their importance in mitigating critical risks such as data breaches, unauthorized access, identity theft, and compliance violations. As a mid-sized organization, SouthernCross may not have the resources to target the Advanced Tier directly, but these domains are still considered critical. Ensuring intermediate-level measures in these domains helps protect patient privacy, maintain trust, and comply with stringent healthcare regulations like HIPAA while balancing resource constraints.

- For **Network Security (NS)** and **Compliance and Legal (C&L)**, they aim for the **Basic Tier**, focusing on establishing foundational practices that can be gradually improved. This foundational tier is chosen because SouthernCross is in the early stages of building basic compliance and network security controls. The organization aims to establish a minimum level of security and compliance first, ensuring essential protections are in place before allocating additional resources to more advanced measures.

Assume there are following practices in each domain.

Risk Management Domain

Tier 1 - Basic		
ID	Practice	Metric (with number of points)
1	Cyber risks are identified, at least in an ad hoc manner.	Frequency of cyber risk identification activities. 0: No cyber risk identification activities are performed. 1: Cyber risk identification is performed annually. 2: Cyber risk identification is performed semi-annually. 3: Cyber risk identification is performed quarterly or more

		frequently.
2	Cyber risks are prioritized based on estimated impact, at least in an ad hoc manner.	Percentage of identified cyber risks that are prioritized based on estimated impact. 0: Less than 50% of cyber risks are prioritized based on impact. 1: 50% to 70% of cyber risks are prioritized based on impact. 2: 71% to 90% of cyber risks are prioritized based on impact. 3: More than 90% of cyber risks are prioritized based on impact.
	Tier 2 - Intermediate	
1	A strategy for cyber risk management is established and maintained in alignment with the organization's cybersecurity program strategy	Degree of alignment between the cyber risk management strategy and the organization's overall cybersecurity program. 0: No alignment. 1: Low alignment. 2: Moderate alignment. 3: High alignment.

Identity and Access Management (IAM) Domain

Tier 1 - Basic		
ID	Practice	Metric (with number of points)
1	Identities are provisioned, at least in an ad hoc manner, for personnel and other entities requiring access.	The number of identities provisioned per defined timeframe. 0: Less than 70% of required identities provisioned within a timeframe. 1: 70%-85% of identities provisioned within the timeframe. 2: 85%-95% of identities provisioned within the timeframe. 3: 95% or more identities provisioned within the timeframe.
2	Logical access controls are implemented, at least in an ad hoc manner	Percentage of logical access controls implemented per department. 0: Less than 70% implementation in required departments. 1: 70%-85% implementation. 2: 85%-95% implementation. 3: 95% or more implementation.
	Tier 2 - Intermediate	
1	Identity repositories are reviewed and updated periodically and according to defined triggers.	Frequency of identity repository updates. 0: Updated less than annually. 1: Updated annually. 2: Updated biannually. 3: Updated quarterly or upon significant organizational change.
2	Logical access requirements incorporate the principle of least privilege	Percentage of logical access privileges aligned with least privilege principle. 0: Less than 70% alignment.

		1: 70%-85% alignment. 2: 85%-95% alignment. 3: 95% or more alignment.

Data Security (DS) Domain

Tier 1 - Basic		
ID	Practice	Metric (with number of points)
1	Establish and maintain data classification.	Percentage of data assets classified. 0: Less than 70% of data assets are classified. 1: 70%-85% classified. 2: 85%-95% classified. 3: 95% or more classified.
2	Define and execute backup and recovery procedures	Frequency of backups conducted for critical data. 0: Backups conducted less than monthly. 1: Monthly backups. 2: Weekly backups. 3: Daily backups.
	Tier 2 - Intermediate	
1	Apply access controls to sensitive data	Percentage of sensitive data with enforced access controls. 0: Less than 70% of sensitive data with access controls. 1: 70%-85% with access controls. 2: 85%-95% with access controls. 3: 95% or more with access controls.

Network Security (NS) Domain

Tier 1 - Basic		
ID	Practice	Metric (with number of points)
1	Implement basic firewall rules on a perimeter network	Percentage of perimeter networks with current firewall rules. 0: less than 70% of networks are protected by firewall rules. 1: 70%-85% protected. 2: 85%-95% protected. 3: 95% or more protected.
2	Enable basic intrusion detection system (IDS) on key network components	Percentage of network components with IDS enabled. 0: less than 70% of components are covered by IDS. 1: 70%-85% covered. 2: 85%-95% covered. 3: 95% or more covered.
3	Deploy regular network traffic logging	Frequency of logging on critical network segments. 0: no logging enabled. 1: monthly logs enabled.

		2: weekly logs enabled. 3: daily or real-time logs enabled.

Compliance and Legal (C&L) Domain

Tier 1 - Basic		
ID	Practice	Metric (with number of points)
1	Identify and track applicable compliance requirements	Percentage of compliance requirements identified and documented. 0: less than 70% identified. 1: 70%-85% identified. 2: 85%-95% identified. 3: 95% or more identified.
2	Establish basic compliance policies and procedures	Percentage of departments with documented compliance policies. 0: less than 70% have documented policies. 1: 70%-85% documented. 2: 85%-95% documented. 3: 95% or more documented.
3	Assign responsibility for compliance-related tasks	Percentage of compliance tasks with assigned responsibility. 0: less than 70% assigned. 1: 70%-85% assigned. 2: 85%-95% assigned. 3: 95% or more assigned.

Assume SouthernCross has implemented the following practices and achieved the following metrics within each domain.

Risk Management Domain

Tier 1 - Basic		
ID	Practice	Metric (with number of points)
1	Cyber risks are identified, at least in an ad hoc manner. 2 points - Fully Implemented	Frequency of cyber risk identification activities. 0: No cyber risk identification activities were performed. 1: Cyber risk identification is performed annually. 2: Cyber risk identification is performed semi-annually. 3: Cyber risk identification is performed quarterly or more frequently. 2 points
2	Cyber risks are prioritized based on estimated impact, at least in an ad hoc manner. 1 point - Partially Implemented	Percentage of identified cyber risks that are prioritized based on estimated impact. 0: Less than 50% of cyber risks are prioritized based on impact. 1: 50% to 70% of cyber risks are prioritized based on

		impact. 2: 71% to 90% of cyber risks are prioritized based on impact. 3: More than 90% of cyber risks are prioritized based on impact. 1 point
	Tier 2 - Intermediate	
1	A strategy for cyber risk management is established and maintained in alignment with the organization’s cybersecurity program strategy. 1 point - Partially Implemented	Degree of alignment between the cyber risk management strategy and the organization's overall cybersecurity program. 0: No alignment. 1: Low alignment. 2: Moderate alignment. 3: High alignment. 1 point

Identity and Access Management (IAM) Domain

Tier 1 - Basic		
ID	Practice	Metric (with number of points)
1	Identities are provisioned, at least in an ad hoc manner, for personnel and other entities requiring access. 2 points - Fully Implemented	The number of identities provisioned per defined timeframe. 0: Less than 70% of required identities provisioned within a timeframe. 1: 70%-85% of identities provisioned within the timeframe. 2: 85%-95% of identities provisioned within the timeframe. 3: 95% or more identities provisioned within the timeframe. 2 points
2	Logical access controls are implemented, at least in an ad hoc manner. 2 points - Fully Implemented	Percentage of logical access controls implemented per department. 0: Less than 70% implementation in required departments. 1: 70%-85% implementation. 2: 85%-95% implementation. 3: 95% or more implementation. 2 points
	Tier 2 - Intermediate	
1	Identity repositories are reviewed and updated periodically and according to defined triggers. 1 point - Partially Implemented	Frequency of identity repository updates. 0: Updated less than annually. 1: Updated annually. 2: Updated biannually. 3: Updated quarterly or upon significant organizational change. 1 point

2	Logical access requirements incorporate the principle of least privilege. 0 points - Not Implemented	Percentage of logical access privileges aligned with least privilege principle. 0: Less than 70% alignment. 1: 70%-85% alignment. 2: 85%-95% alignment. 3: 95% or more alignment. 0 points

Data Security (DS) Domain

Tier 1 - Basic		
ID	Practice	Metric (with number of points)
1	Establish and maintain data classification. 2 points - Fully Implemented	Percentage of data assets classified. 0: Less than 70% of data assets are classified. 1: 70%-85% classified. 2: 85%-95% classified. 3: 95% or more classified. 3 points
2	Define and execute backup and recovery procedures. 1 point - Partially Implemented	Frequency of backups conducted for critical data. 0: Backups conducted less than monthly. 1: Monthly backups. 2: Weekly backups. 3: Daily backups. 2 points
	Tier 2 - Intermediate	
1	Apply access controls to sensitive data. 1 point - Partially Implemented	Percentage of sensitive data with enforced access controls. 0: Less than 70% of sensitive data with access controls. 1: 70%-85% with access controls. 2: 85%-95% with access controls. 3: 95% or more with access controls. 1 point

Network Security (NS) Domain

Tier 1 - Basic		
ID	Practice	Metric (with number of points)
1	Implement basic firewall rules on perimeter network 1 point - Partially Implemented	Percentage of perimeter networks with current firewall rules. 0: less than 70% of networks are protected by firewall rules. 1: 70%-85% protected. 2: 85%-95% protected.

		3: 95% or more protected. 1 point
2	Enable basic intrusion detection system (IDS) on key network components 0 points - Not Implemented	Percentage of network components with IDS enabled. 0: less than 70% of components are covered by IDS. 1: 70%-85% covered. 2: 85%-95% covered. 3: 95% or more covered. 0 points
3	Deploy regular network traffic logging 2 points - Fully Implemented	Frequency of logging on critical network segments. 0: no logging enabled. 1: monthly logs enabled. 2: weekly logs enabled. 3: daily or real-time logs enabled. 3 points

Compliance and Legal (C&L) Domain

Tier 1 - Basic		
ID	Practice	Metric (with number of points)
1	Identify and track applicable compliance requirements 1 point - Partially Implemented	Percentage of compliance requirements identified and documented. 0: less than 50% identified. 1: 51%-70% identified. 2: 71%-90% identified. 3: 91% or more identified. 1 point
2	Establish basic compliance policies and procedures 1 point - Partially Implemented	Percentage of departments with documented compliance policies. 0: less than 70% have documented policies. 1: 70%-85% documented. 2: 85%-95% documented. 3: 95% or more documented. 1 point
3	Assign responsibility for compliance-related tasks 0 points - Not Implemented	Percentage of compliance tasks with assigned responsibility. 0: less than 70% assigned. 1: 70%-85% assigned. 2: 85%-95% assigned. 3: 95% or more assigned. 0 points

The calculation of the scores and the maturity level is as follows for each domain.

Risk Management (RM) Domain

Practice Implementation Score = ((2+1) + (1))/(2 x (2+1)) x 100 = 0.667 x 100 = 66.7%

Metric Achievement Score = ((2+1) + (1))/(3 x (2+1)) x 100 = 0.444 x 100 = 44.4%

Domain Score = (66.7+44.4)/2 = 55.6%

Domain Maturity Level - Managed

Identity and Access Management (IAM) Domain

Practice Implementation Score = ((2+2) + (1+0))/(2 x (2+2)) x 100 = 62.5%

Metric Achievement Score = ((2+1) + (1+0))/(3 x (2+2)) x 100 = 33.333%

Domain Score = (62.5+ 33.333)/2 = 47.92%

Domain Maturity Level - Managed

Data Security (DS) Domain

Practice Implementation Score = ((2+1) + (1))/(2 x (2+1)) x 100 = 66.667%

Metric Achievement Score = ((3+2) + (1))/(3 x (2+1)) x 100 = 66.667%

Domain Score = (66.667+66.667)/2 = 66.67%

Domain Maturity Level - Managed

Network Security (NS) Domain

Practice Implementation Score = ((1+0) + (2))/(2 x 3) x 100 = 50%

Metric Achievement Score = ((1+0) + (3))/(3 x 3) x 100 = 44.444%

Domain Score = (50+44.444)/2 = 47.22%

Domain Maturity Level - Managed

Compliance and Legal (C&L) Domain

Practice Implementation Score = ((1+1) + (0))/(2 x 3) x 100 = 33.333%

Metric Achievement Score = ((1+1) + (0))/(3 x 3) x 100 = 22.222%

Domain Score = (33.333+22.222)/2 = 27.78%

Domain Maturity Level - Initial

Based on the domain scores calculated above and weights identified for each domain the overall maturity score is calculated as follows.

Assuming that the weights for each domain are as follows,

- RM - 0.25
- IAM - 0.20
- DS - 0.25
- NS - 0.15
- C&L - 0.15

Overall Maturity Score = (55.6 x 0.25) + (47.92 x 0.20) + (66.67 x 0.25) + (47.22 x 0.15) + (27.78 x 0.15) = 51.402%

Overall Maturity Level - Managed

The results of the maturity assessment indicate a consistent level of "Managed" maturity across most domains, with the exception of Compliance and Legal (C&L), which remains at the "Initial" level. Notably, the Risk Management (RM), Identity and Access Management (IAM), Data Security (DS), and Network Security (NS) domains each demonstrate significant practice implementation and metric achievement, with scores ranging from 47.22% to 66.67%, reflecting structured and partially consistent processes. However, Compliance and Legal, with a domain score of 27.78%, highlights the need for foundational improvements to elevate compliance practices and legal safeguards.

Aggregating the weighted scores across all domains yields an overall maturity score of 51.4%, classifying the organization's cybersecurity capability as "Managed." This indicates that, while processes and controls are generally established and monitored, they could benefit from further consistency, rigour, and standardization, especially within the C&L domain. Moving forward, targeted improvements in the Compliance and Legal domain, along with continuous refinement across other areas, would enhance the organization's cybersecurity capability and elevate its overall maturity level.