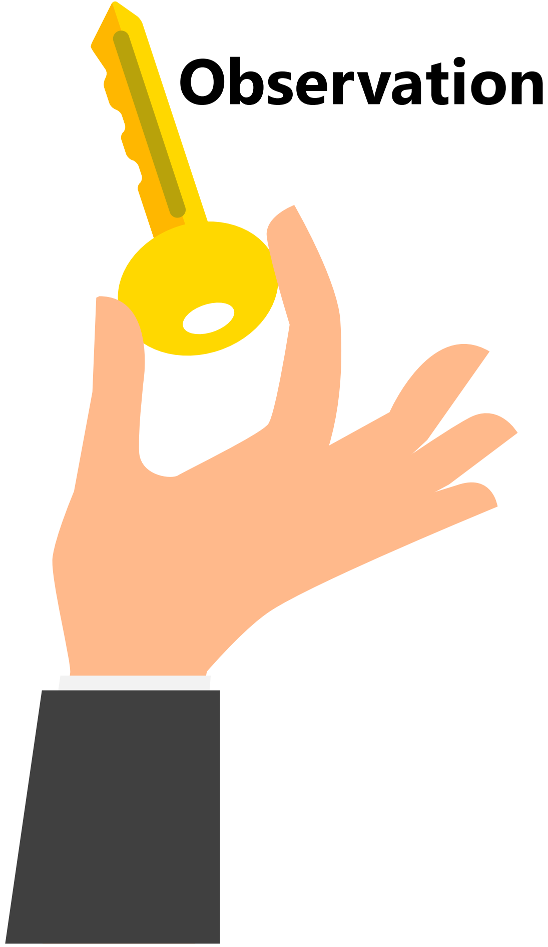
CISO’s – First 100 Days Roadmap

Your success as a security leader is determined largely by your first 100 days in the role.



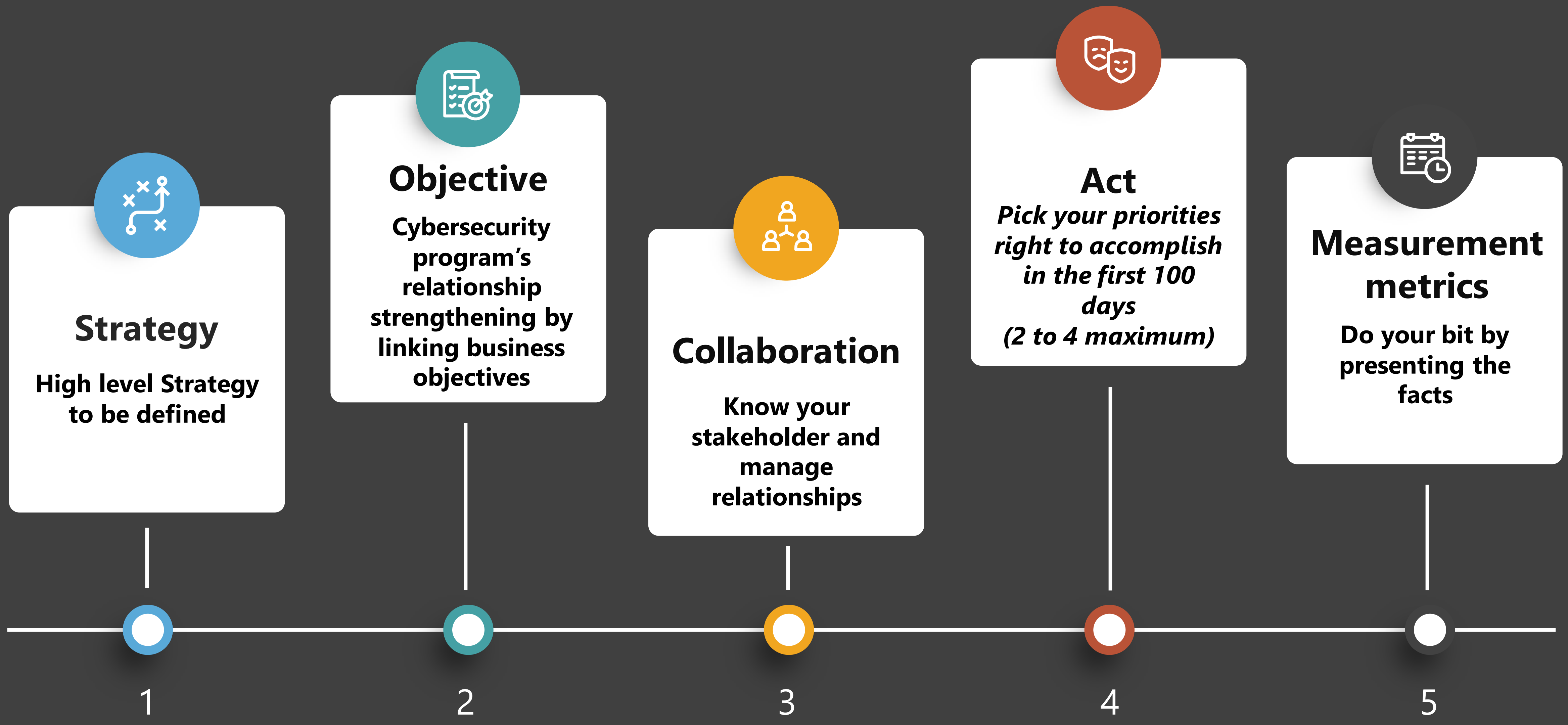
Observations

For a CISO (chief information security officer) to be successful is required to be good communicator, leadership aspects when it comes to giving directions and most importantly, good listeners & not just technologists.

The success of a CISO is by having to establish the foundation right for the security program and ensuring personal credibility across the organization.

New CISO’s will struggle when they do not understand the leadership expectations or fail to be a business enabler by demonstrating results effectively.

CISO’s – First 100 Days Roadmap



1

Strategy

High level Strategy to be defined

2

Objective

Cybersecurity program’s relationship strengthening by linking business objectives

3

Collaboration

Know your stakeholder and manage relationships

4

Act

Pick your priorities right to accomplish in the first 100 days (2 to 4 maximum)

5

Measurement metrics

Do your bit by presenting the facts

Plan – Strategy

- **Assess the type of CISO that your organization needs** because every organization has a culture, political challenges and many such other aspects. An organization may need a operationally driven CISO or more business driven one
- **Creative ways of working - Storytelling is an effective way** to gain acceptance by making the stakeholders understand that how CISO can help enable business without compromising on security
- **Identify key stakeholders** the C–Suite and their priorities and expectations of you.
- Go through the **organization charts and operational documents** (e.g., process maps) to understand the structure of security, IT and the overall enterprise.
- **Talking to your own security team** by understanding the current structure, security governance, priorities, automation, support they require and challenges.

Outcomes

- A **relationship tracker** for all the basic engagement plans to meet leadership stakeholders and your team
- A common **understanding of your role and the expectations** of your staff, senior stakeholders and leadership team.
- This phase focuses on **listening and learning — not decision making**.
- Unless its some thing which cannot wait , lets **avoid making any announcements or taking decisions** in your first few weeks.

Initial Objectives

- **One critical objective is to have a senior level mentor** who need not be a security expert however look for someone who has insights to organization culture and shares realistic objectives and shares the feedback on for how your proposal and leadership is acknowledged
  - **Define security's roles and responsibilities** which clarifies the ownership across different domains within Info Sec and for areas outside security's responsibility, ensure you develop working relationships leaders across different departments.
    - **Prepare a catalog of all your information sources**, like the organization charts, policies , current priorities, technology roadmaps as this will be useful to determine the current state and immediate plans.
      - **Start with a maturity assessment** spanning different areas like the functional maturity assessment, audit findings, Vulnerability assessments, Threat assessments, Talent assessments, Regulatory findings, Penetration tests etc.
        - **Security improvement areas to be identified** post assessment, ensure you have a strategic list of priorities

Outcomes

- **Security improvement areas** identified during the maturity assessments, team conversations and engagements with C-Suit
  - A **select list of top 3 to 5 security improvement areas identified** and which are inline to business goals and strategy.
    - **Identify team resources available** which includes and not limited to funding, headcount, technology automation.
      - An **executive mentor that provides insight** into the culture of the enterprise.

Collaboration - IT, Marketing or Products

For the selected 2-3 security improvement areas to focus on over the next three months:

It's recommended to **choose the priorities** based on the below criteria:

- Can the initiative be achieved within three months?
- Will you have the required executive support, resources and budget?
- Is the initiative addressing the top challenge of the organization (risk reduction)?
- Is the risk of failure and is that low?

Which other departments – like the Products/Marketing or IT support would you need to accomplish this priorities?

Outcomes

- **Teams responsible and support required** from departments identified.
- **Budget requirements** from operational perspective, resource allocation and support priorities.
- **Target** "Where we would like to be", "Where we are currently" and "How will be get there"

Act -Implementation

- **Present your strategic plan and vision** to leadership and stakeholders across the organization. Ensure you have tailored the message for different stakeholders as per the support you may need from the leadership team.
- **Building an effective information risk governance,** which includes risk decision-making rights, risk accountability and proper risk ownership.
- **Security managers must have well-defined roles and responsibilities**, the security staff have a clear responsibilities description and target which are measurable as a part of performance management and metrics which can demonstrated to the stakeholders.
- **Securing the support and budget required achieve the set targets**. Ensure there are dashboards which are presented to the leadership to give an update , assurance that we are on the right track and gain confidence of the board of directors, management and fellow department heads.

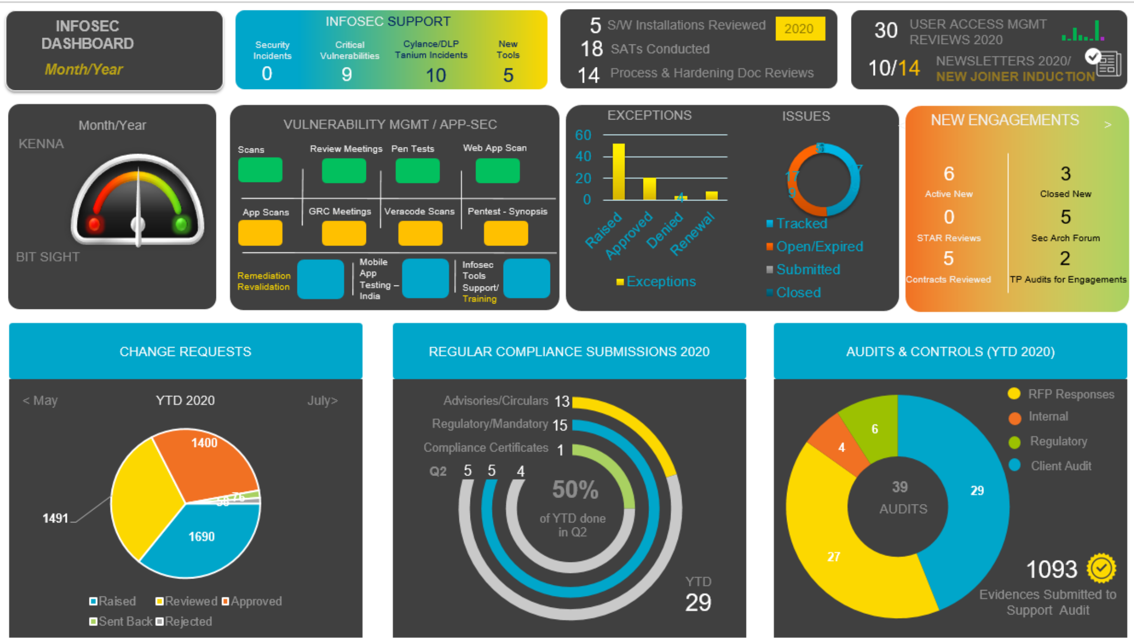
Outcomes

- Series of scheduled **meetings with security managers, staff and other stakeholders**.
- **Project owner for each of the identified security improvement areas** identified as security's top priorities.
- A **security budget allocation** across resources (people, process and technology)
- A list of **tangible and measurable project results** that demonstrate progress against your strategic objectives.

Measurement Metrics

- **Track the progress** of all the security improvement areas identified during the assessment phase, report progress to leadership, and use this momentum to make the business case for other areas identified for a continuous improvement of security posture.

  - **Articulation of the metrics** is important and needs to talk the business language for the relevant teams (how priorities are mapped and support the organization's business objectives).



  - **Communication is important** whether they are wins or challenges and identifying solutions to address challenges as they emerge. As an experience almost all security initiatives have multiple targets (some smaller, some larger) — and we must communicate to all even if some goals are delayed or missed and may be achieved.

Outcomes

- **An established meeting and reporting cadence** for various stakeholders, including the CIO, risk steering committee, C-suite and board

  - **Evidence of early progress** to be reported to stakeholders and the leadership team.

    - **A defined set of operational metrics** to track performance and progress across security initiatives.