RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **RMG-M02**

The Zoom Effect: A Framework for Security Program Transformation

Ariel Chavan

Head of Security Product and Program Management

Zoom Video Communications, Inc.

Heather Ceylan

Head of Security Standards, Compliance, and Customer Assurance

Zoom Video Communications, Inc.

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA® Conference, RSA Security LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

RSAConference2022

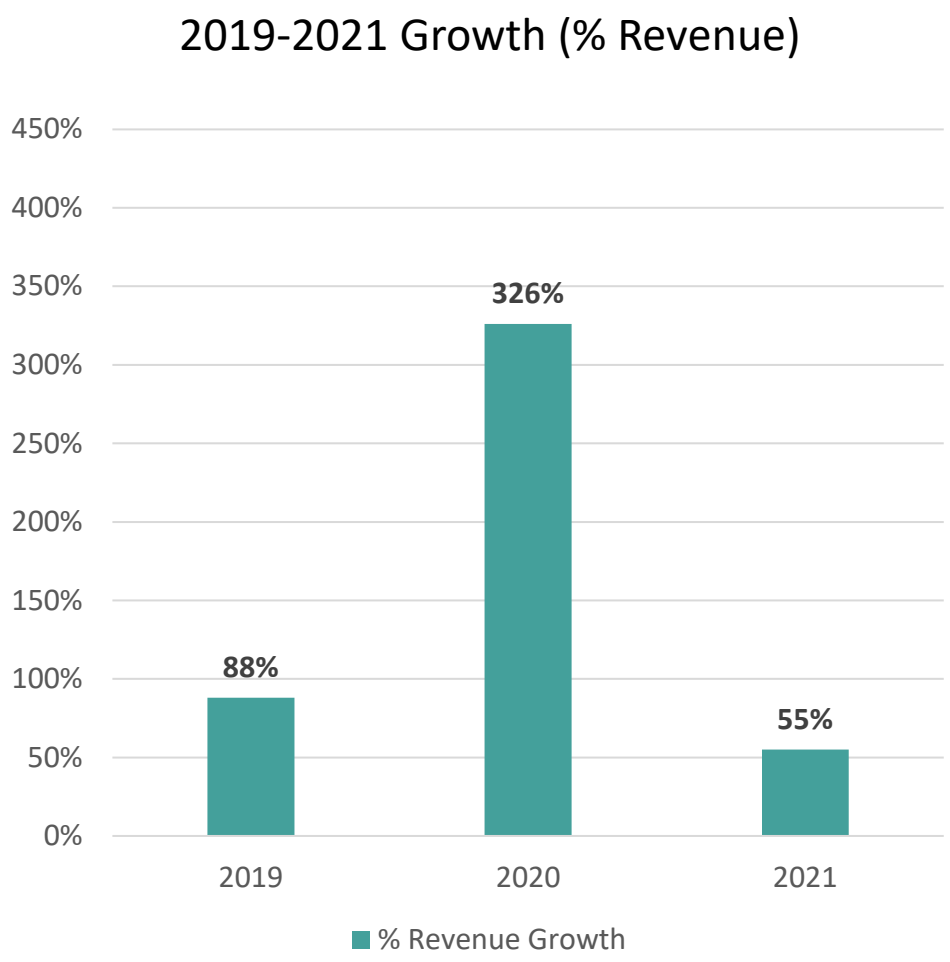
Introduction

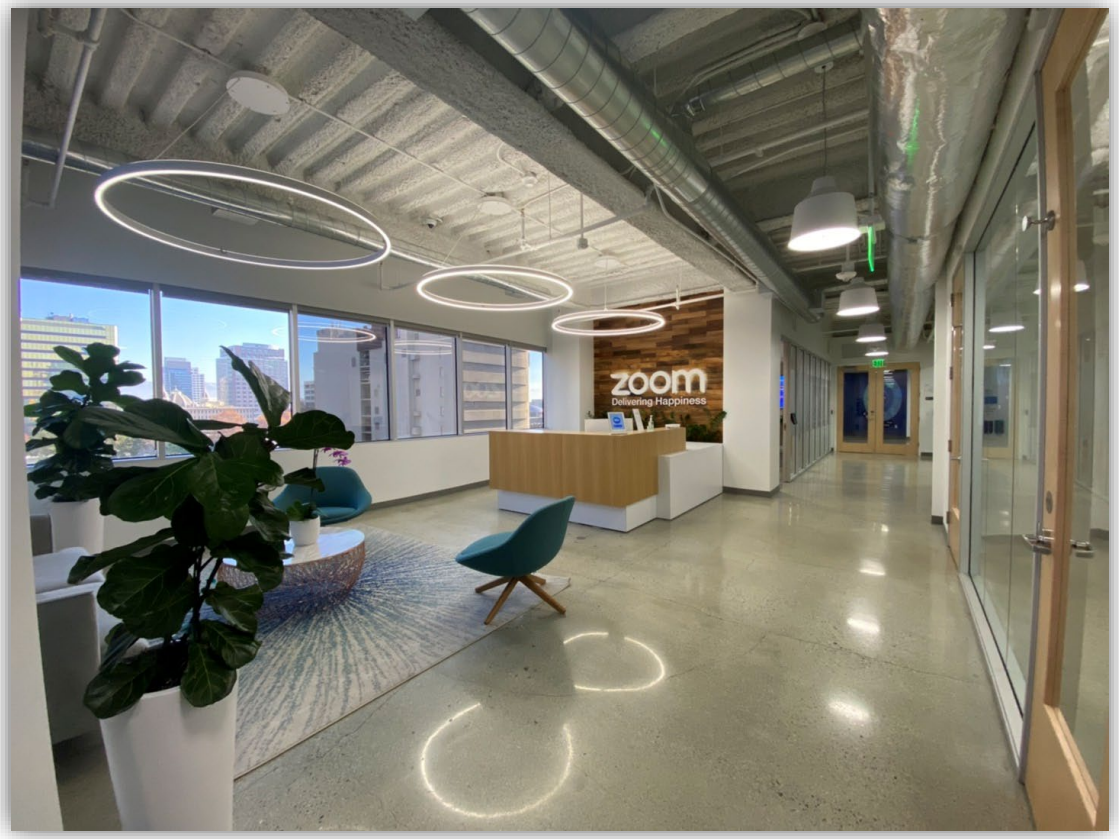
Zoom Snapshot: Pre-Pandemic

In December 2019, Zoom meetings reached **10 million** daily meeting participants, free and paid.

By April 2020, that number peaked at **300 million**.

Unprecedented Growth



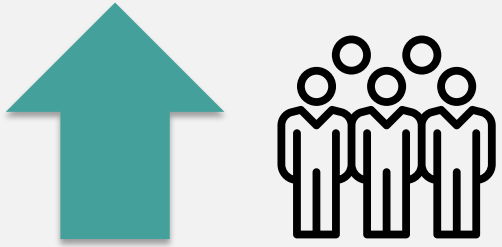


Need for Transformation Framework

- **Communication.** With the rapid pace of hiring and team formation, we needed a structure for effective onboarding, communication, and team alignment.
- **Focus.** We needed to make sure teams were focused on the right priorities and that our priorities were being driven by business risk.
- **Resources.** We needed mechanisms to determine and justify resource needs.
- **Measurement.** We needed to ensure mechanisms were in place to measure and report on progress of the security program.

What Happened When We Applied the Transformation Framework

Security Team Headcount



200+

Program Effectiveness

25%

Other Outcomes:

- Implemented new organizational structure
- Increased visibility and transparency between security and partner organizations resulted in improved alignment on priorities
- Increased security awareness and engagement across the company

Session Goals

- Provide a general framework that can be adapted to rapidly transform, scale, or improve your security program
- Learn how to utilize the framework to:
  - Obtain cross-functional executive and board support
  - Justify budget and resourcing requirements
  - Communicate and align objectives and priorities
  - Measure and communicate progress
  - Ensure appropriate governance and accountability
- Share lessons learned and key factors to consider when building or adapting your framework

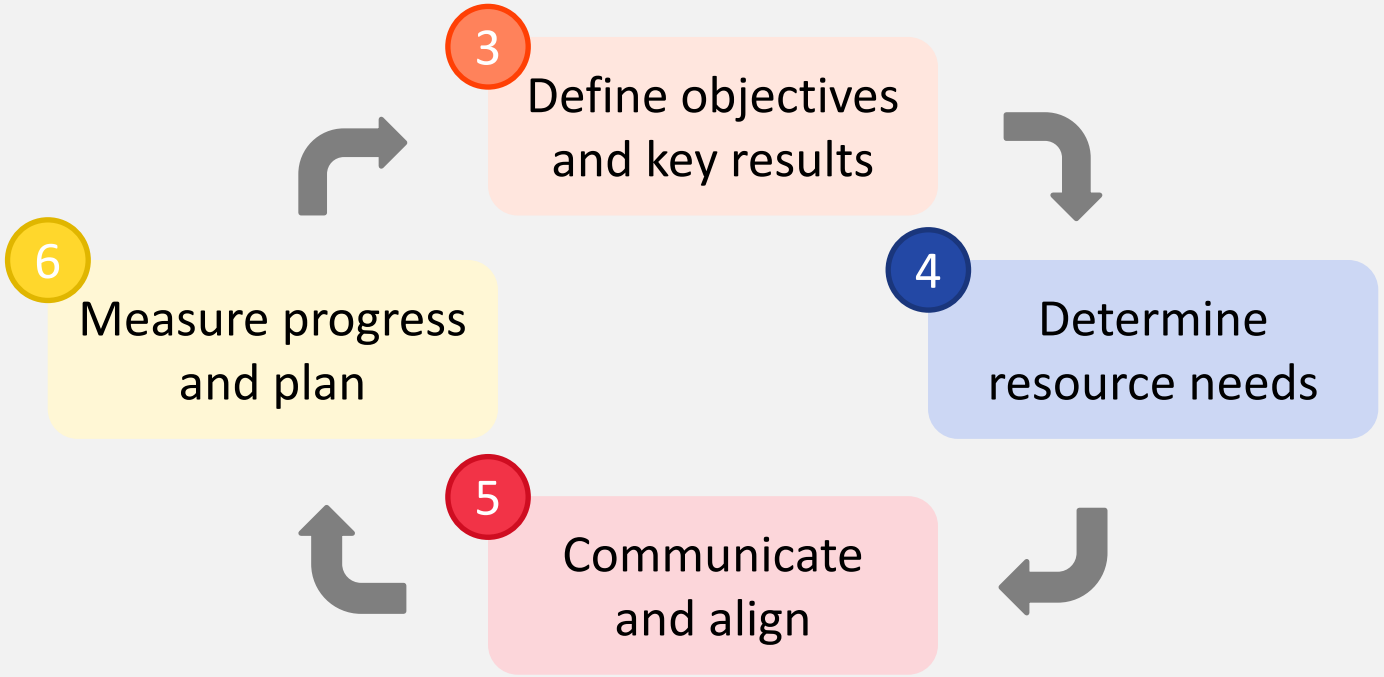
RSAConference2022

Transformation Framework

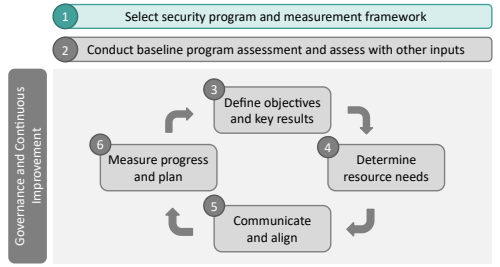
Transformation framework overview

1. Select security program and measurement framework
2. Conduct baseline program assessment and assess with other inputs

Governance and Continuous Improvement



1. Select security program and measurement framework



Considerations

- What are we trying to achieve?
- Is maturity the right measurement?
- How will the framework resonate in communications with the board and non-security stakeholders?
- How will the framework resonate with external stakeholders, auditors, and regulators?

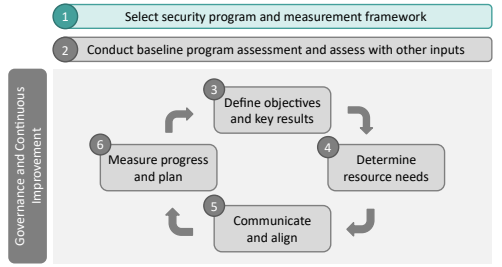
Common Security Program Frameworks

- NIST Cybersecurity Framework (CSF)
- ISO 27001
- HITRUST CSF

Common Measurement Frameworks

- NIST CSF
- Capability Maturity Model Integration (CMMI)
- HITRUST CSF

1. Select security program and measurement framework



Where we landed:

Governance
(ISO 27001)

- Objectives and Key Results
- Budget and Resource Planning
- Communication and Awareness
- Documentation

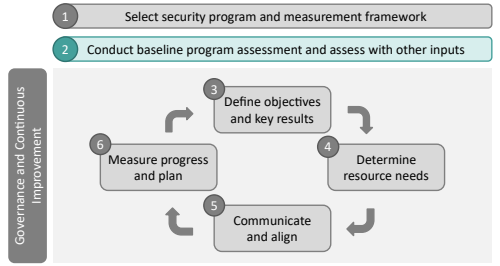
Security Framework
(NIST CSF)

Identify	Protect	Detect	Respond	Recover
• Asset Mgmt. • Business Env. • Governance • Risk Mgmt. • Supply Chain	• IAM • Awareness • Data Security • Data Protection • Maintenance	• Anomalies • Cont. Monitoring • Detection	• Response Plan • Comm's • Analysis • Mitigation • Improvements	• Recovery Plan • Improvements • Comm's

Continuous Improvement
(ISO 27001, NIST CSF)

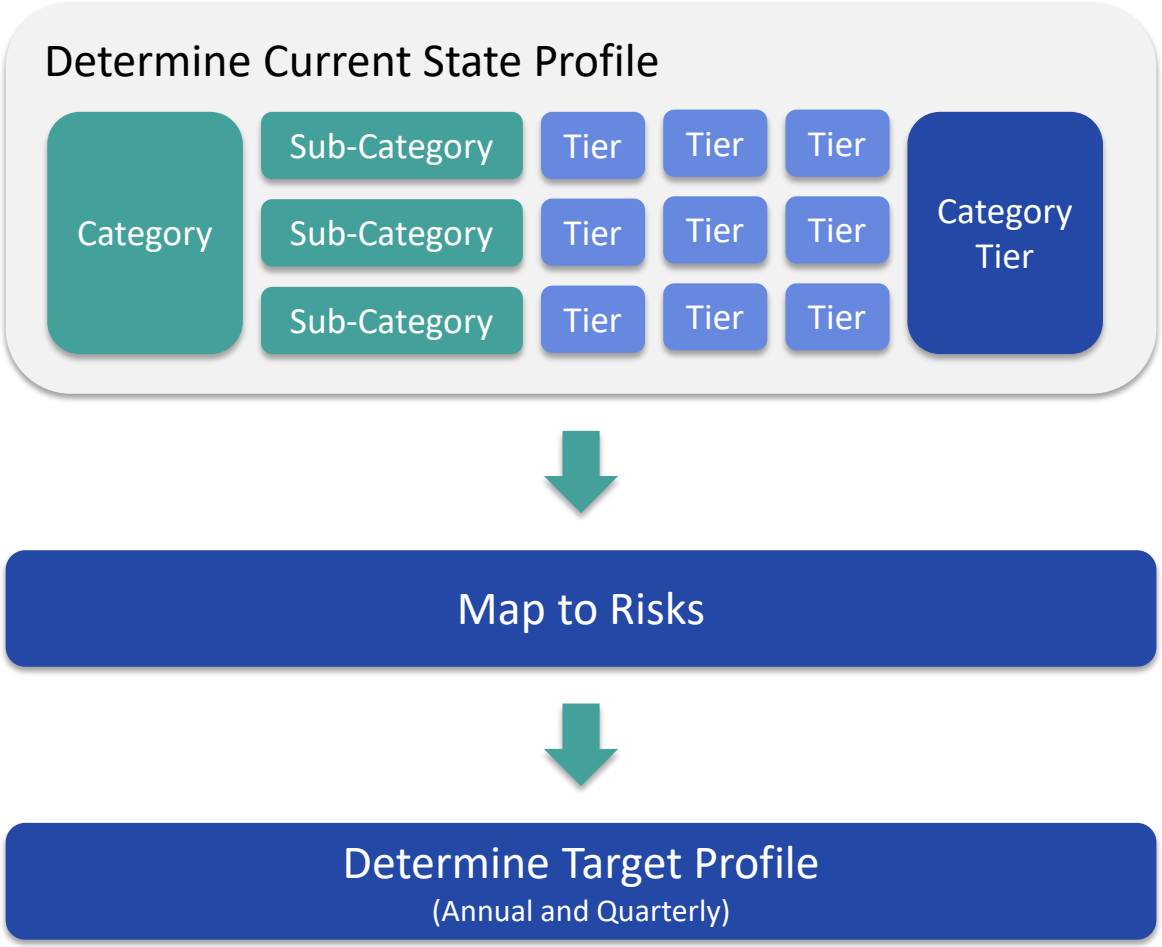
- Measurement and Evaluation
- Executive and Board Review
- Continuous Improvement

2. Conduct baseline program assessment

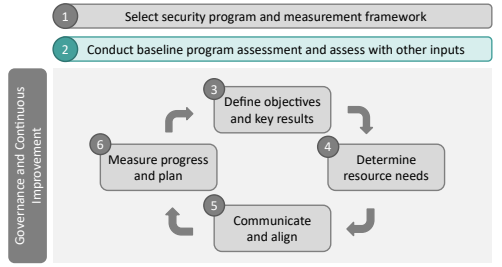


Considerations

- What are the goals of the assessment?
- Who will conduct the assessment?
- How will the assessment be conducted?
- How frequently will we conduct assessments?



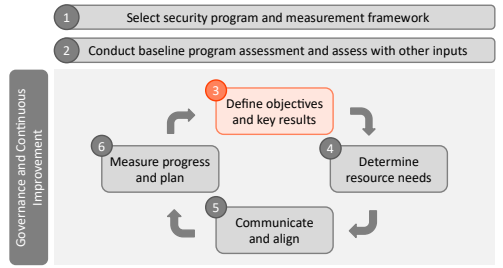
2. Assess with other inputs



Program Assessment + Risk Assessments + Business Objectives + Compliance Requirements

Security Program Priorities and Objectives

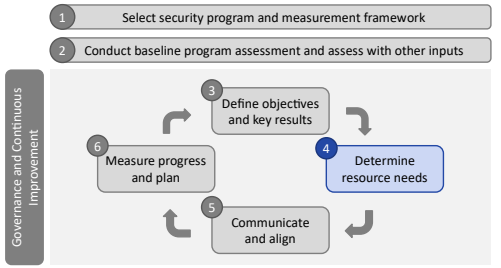
3. Define Objectives and Key Results



Objective and Key Result Example:

CISO Objectives *(Strategic)*	Build and operationalize foundational security capabilities to identify, prevent, and detect threats and vulnerabilities
Functional Area Objectives *(Aspirational)*	Increase consumer safety by reducing company's attack surface
Key Result *(Measurable)*	x% of vulnerabilities remediated within SLA
Key Result *(Measurable)*	x% of assets that are covered by configuration benchmark scans
Key Result *(Measurable)*	x% of vulnerabilities are automatically routed to partners via tickets
Initiatives *(achievable)*	Validate central asset management system by the end of Q4
Initiatives *(achievable)*	Deploy and operationalize configuration scanning tool by the end of Q3
Initiatives *(achievable)*	Automate assigning to asset owning teams for remediation by Q3

4. Determine resource needs



Fiscal Year Planning

Review OKR Initiatives → What can we accomplish with existing resources? → Where do we need additional resources? → Security Leadership Review → Executive Leadership Review

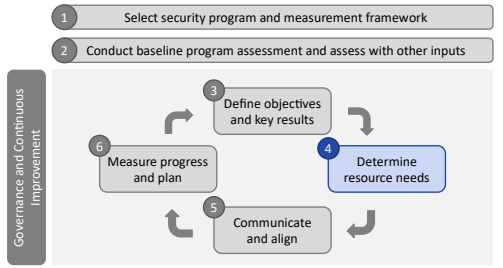
Business Partner Reviews

Quarterly Resource Review

Have priorities changed / not progressing as planned? → Security Leadership Review → Executive Leadership Review

Business Partner Reviews

Zoom's Security Functions



Chief Information Security Officer

Engineering Security

Security Operations

Security GRC and Perf. Mgmt.

Enterprise Security

Security Strategy and Management

Detection and Response

Phys. Sec. and Bus. Resilience

Offensive Security

Vuln. Mgmt. Bug Bounty

Product Security

Technical Compliance

Security Legal

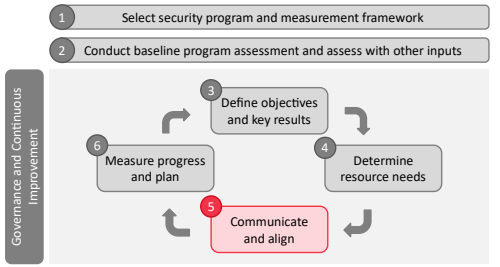
Insider Risk

IT

Product Engineering

Privacy

5. Communicate and align with key stakeholders



Considerations

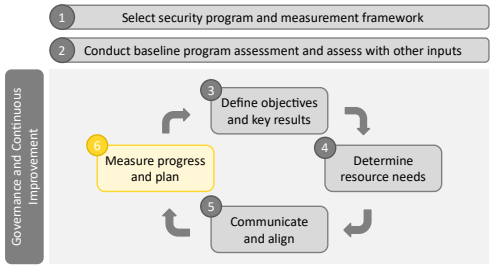
- How do you communicate effectively across all levels?
- What is the purpose of each venue for information communication?
- What is the desired output and to who?
- What is the right medium or tool to communicate?

Monthly Business Reviews

Quarterly Business Reviews

Quarterly Board Meetings

6. Measure progress and re-plan



Measurement Against Objectives (Progress)

- Are the objectives still in alignment with business priorities and risks?
- What is the measurable progress against each key result supporting the metric?
- Are changes required to set more realistic or achievable objectives?

Monthly Business Reviews

Quarterly Business Reviews

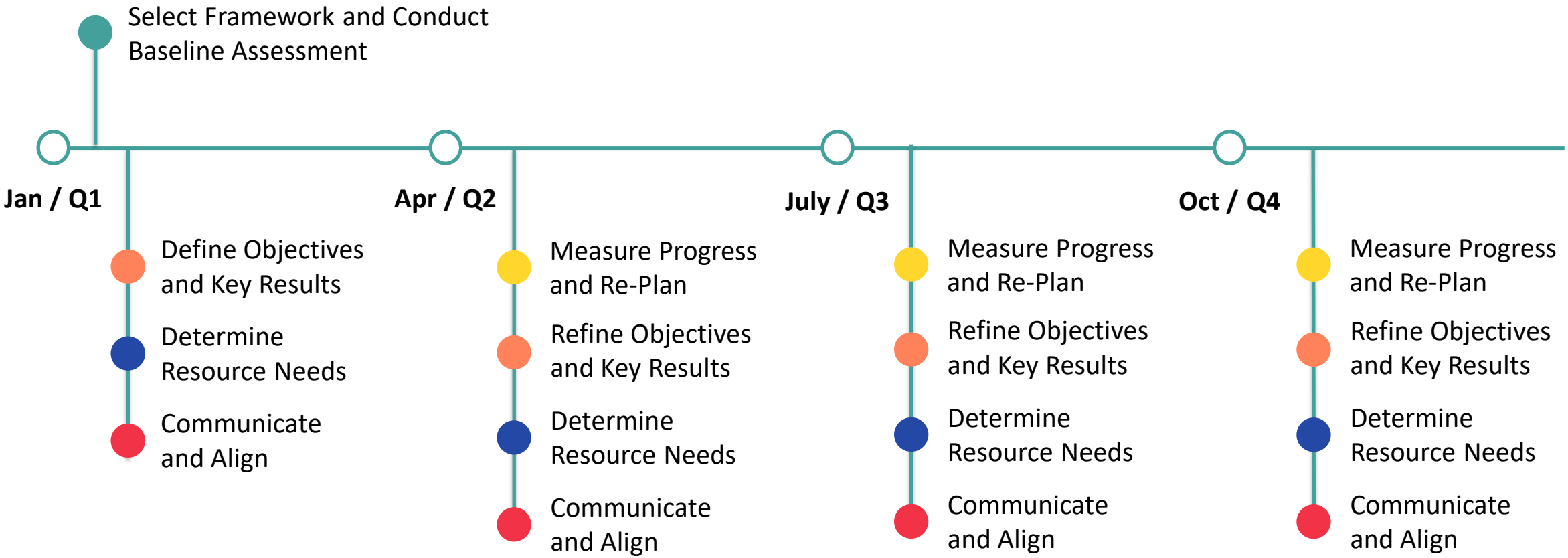
Measurement Against Framework (Effectiveness)

- What is the expected end target based on set out plans for the year?
- How can this be broken out and measure progress quarter by quarter?
- How well is the organization progressing in maturing our security controls across?

Quarterly Internal Assessments

Annual Independent Assessments

Example Rhythm of Business



RSAConference2022

Applying What You've Learned Today

Summary of Lessons Learned

- **Security as a Company-Wide Program** - Ensure input from and alignment with supporting departments and stakeholders
- **Take Program Assessment in Context** - When determining objectives and priorities, consider multiple inputs, not just the baseline and target program assessment
- **Communicate the "Why"** - Understand and communicate the "why" behind the target state – tie target state back to organization-specific risks
- **Allow for Scale** - Create documentation and educational materials to support rapid team growth and scale
- **Collaboration Tools** - Have the right tools for cross-functional collaboration and visibility
- **Create Flexibility** - Allow flexibility in the framework to adjust for program scale

Applying what you've learned today

- Next week you could:
  - Understand where your security organization is in the journey – building, stable/steady growth, undergoing transformation
- In the first three months following this presentation you could:
  - If you are building/transforming, establish security program and governance framework, taking into account considerations and lessons discussed today
  - If you are stable/steady growth, evaluate your current security program and governance framework and identify opportunities for improvement and scale
- Within six months you could:
  - Implement core elements of the framework and conduct baseline and target assessment
  - Continue to implement and mature framework, using lessons learned at your organization

RSAConference2022

Q&A