SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Security Program Strategy & Operations > Strategic Planning/Management >

Universe Assessment Identifies Gaps and Opportunities

By the Security Executive Council

At the Security Executive Council's May 2022 State of the Security Industry (SSOI) Briefing, SEC staff and faculty led participating Tier 1 security leaders through the new Security Success Universe Assessment, designed to help them identify gaps, find credible organizational partners, and enhance security offerings to fit the needs of their organizations.

The SEC Security Success Universe is based on more than 15 years of research into successful security programs and leaders. It outlines 115 elements in 13 categories that can help the security leader down the path to excellence. (Click here to view a graphic of the full Success Universe complete with all subcategories.) SEC staff and faculty selected a few elements under each category to expand upon and shared their insights on how each can contribute to success.

Read on for highlights and to find out how to schedule your own free universe assessment.

Foundational Concepts

1. Security is aligned with the Enterprise Risk Assessment or similar approach
2. Program considers current conditions, circumstance, culture, and resources
3. Organizational readiness, program maturity, and leadership approach are assessed and provide the correct fit.

Bob Hayes, SEC Managing Director: "You're only as strong as your foundation. Make sure your work and your security risks are aligned with the risks the company has identified as critical to their success as a business. And quit worrying about what everybody else is doing. Understand your C4R – your current conditions, circumstance, culture, and resources – because these will help you determine which of your efforts is most likely to be effective."

Risk Identification

1. Risk ownership is determined and agreed upon
2. The organization's risk appetite has been quantified
3. A security risk assessment has been conducted
4. Risk score – mitigation value = residual risk

Tom Bello, Emeritus Faculty (former affiliation, Exxon Mobil Corporation): "When you say a risk assessment has been conducted, do you mean little 'r.a.' or big 'R.A.'? If the back door is broken and the alarm won't work, we're not doing a Risk Assessment on that. When would we conduct a Risk Assessment? When there's a significant change in threat, business consequence, major incident, new project milestone, a significant change in headcount or business footprint, or prior to a divestiture or startup."

Governance/Guidance

1. The security program meets applicable accreditation
2. There is an established minimum baseline security program
3. There is adequate stakeholder guidance documentation
4. The security program has aligned and is compliant with industry standards

Francis D'Addario, Emeritus Faculty, Strategic Innovation (former affiliation, Starbucks Coffee Company):
"It doesn't matter which country you're headquartered in – you have to be locally relevant and responding to national standards and you have to understand you're meeting international expectations. How well we meet or exceed these expectations is measurable, and it's typically audited."

Risk Mitigation

1. Senior leadership has understanding and support of asset protection strategies/measures (info, people, facilities, systems, etc.)
2. Financial loss prevention measures have been implemented
3. New and emerging markets are assessed, and mitigation strategies implemented

Matt Giese, Emeritus Faculty (former affiliation, Fidelity Investments): “It’s important that security’s role in mitigating risk is visible to senior leadership, and to me that’s best accomplished through a dual approach – at the outset, as new senior leaders come on board, having a briefing deck and dialogue ready that introduces security to new leaders including security’s role and key risks that security owns; and on an ongoing basis, engaging senior leaders with clear and compelling key risk indicators and key performance indicators that highlight both successes and challenges.”

Executive Influence

1. You effectively communicate risk with the senior leadership team
2. Security value story is developed to communicate with senior leadership

Dan Sauvageau, Emeritus Faculty (former affiliation, Fidelity Investments): “How do you convey enterprise risk? The wins you’ve experienced? The challenges you’re seeing and overcoming? How often are you conveying this? I would say at least twice a year – not just to a few but to all senior business leaders. Business lines may come to security’s defense when the budget axe is swinging if they know its importance and value to them.”

Organizational Structure

1. There is a defined and agreed upon budget for security responsibilities
2. Reporting relationships are clearly defined
3. A service delivery model has been decided upon with senior leadership support

Dan Sauvageau: “If you have a function that’s embedded in another function, try the best you can to have a clarified, defined budget of security responsibilities. If you have distributed campuses, does your local security head report solid line or dotted line to the local business head? It’s important for transparency and objectivity that that line goes solid line back to security and dotted line to the senior leaders.”

Organizational Management

1. Relevant cross-functional roles and responsibilities are identified and understood
2. There is a defined security organization management structure
3. The strategic plan is aligned with business goals and objectives

Tom Bello: “Always think about who’s going to be affected by what you plan to do. In many cases, HR, Law, Procurement, Audit, are also providing risk management guidance to leadership on different subjects. Their job is to help manage risk just like you. You need to work with them, and sometimes have a difficult discussion with other functional leads and say, here's what we do and here's what you do."

Budget Management

1. Cost avoidance opportunities have been identified and measures implemented
2. Executive management and security have agreed upon return-on-investment criteria.
3. Value-add contributions from security are identified and measured

George Campbell: "Return on security investment is sometimes elusive. Use your CFO as a mentor in building your security ROI strategy into your processes and the annual business plan. They can help you direct and learn about how they approach the notion of ROI and how it can be applied to your service suite."

Program Implementation

1. There is adequate documentation for enterprise scalability
2. Executive management and business units are familiar with and support program implementation plan
3. Appropriate stakeholders have received adequate training

Liz Lancaster-Brisson, M.C.J., Director of Tier 1 Leader Services & Projects: "When we talk about adequate documentation for enterprise scalability, we talk about governance, policy and procedure that will drive this. Do you have documentation that shows you're scalable, repeatable, defensible, and that you can continually be optimizing or improving performance? Don't make documentation an afterthought. It's time consuming, but it's very important."

Talent Management

1. There is an organizational career development plan for team members
2. The recruitment and selection program includes high-potential, entry level candidates
3. Succession planning is in place and utilized

Dean Correia, Emeritus Faculty, Business Continuity Leader (former affiliation: Wal-Mart Canada Corp.): "One of the best ways to defend your organizational structure, influence executives, and get your program implemented is through your team. Making sure your team and you yourself are constantly developed and challenged is crucial to the success of the enterprise. Work with your HR and organizational development partners and even if the structure for talent management isn't in place, put it in place. If it is, strengthen it."

Optimized Operations

1. Stakeholders and customers play an appropriate role in securing their organization
2. Measurements and metrics for operational excellence are in place
3. Quality and accuracy metrics are valued and utilized

George Campbell: "Optimizing can't happen without measurement and metrics. Tell the value story. Script in the data. Don't just count, measure, and show the results of the organization's investments. Build measures into every program. This is not about the numbers; it's about improving efficiency and performance."

Defense and Validation

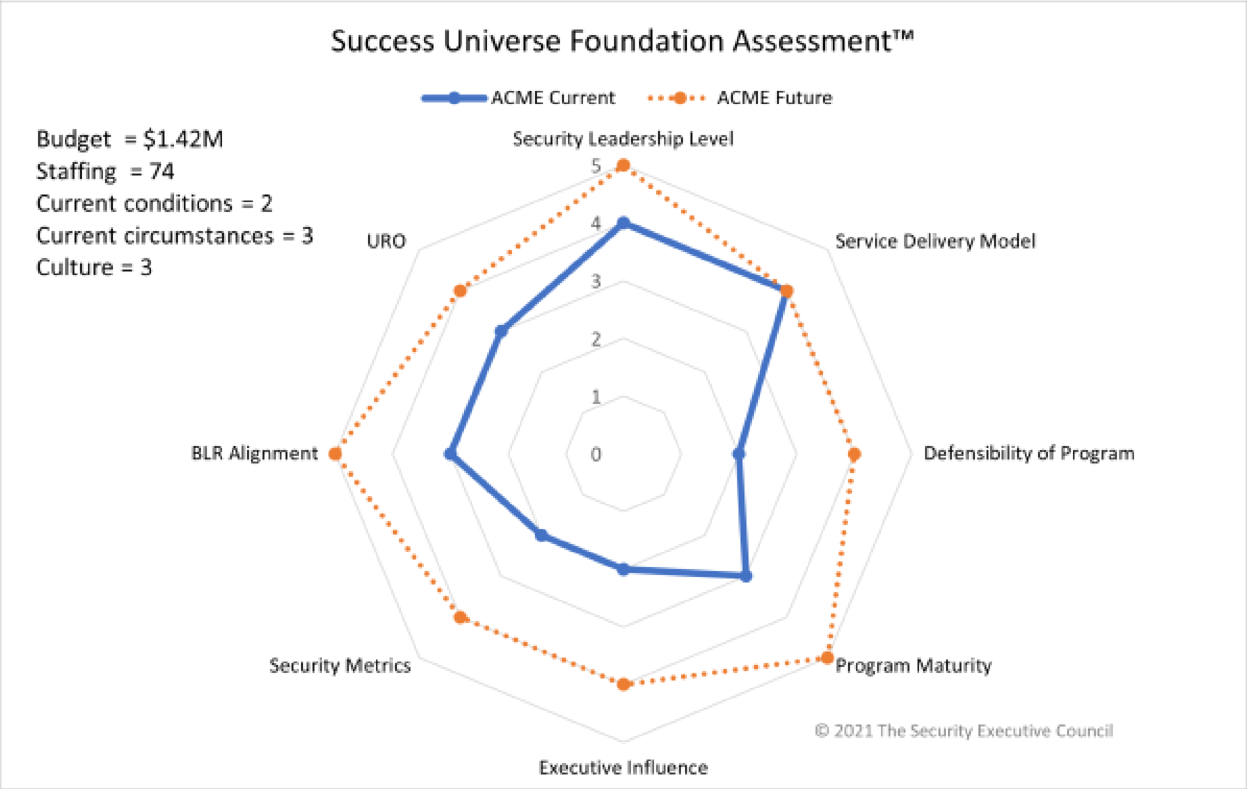
1. Stakeholder and customer confidence surveys are conducted
2. The internal impact and value of the organization is measured, analyzed, and improved upon

Francis D'Addario: "How confident are our stakeholders, on a 1 -10 scale, in our people, acumen, resources, and technology to mitigate the all-hazards risks that will affect your business? Then follow up by asking what it will take to improve their confidence in our ability to mitigate those risks? Be thoughtful, considerate, and responsible."

Programs

Bob Hayes: "We have a list of 20 programs the CSO can have responsibility for. If you don't own some of these, it's useful to think about who does. Can your security team add value to it? How? Don't just mark it off as outside your purview. Look at it more broadly - don't get rooted deeply into past practices."

After walking through the Security Success Universe assessment, SSOI participants were invited to submit their results to the SEC and receive a spider chart that provides an impactful visual showing where their security program currently is and where it wants to be.



The Security Universe Assessment can show security leaders what is possible for their function. It can help expand your thinking about what you do and what you could do, can help find and analyze gaps, and help to strengthen your program.

It's also a valuable tool for discussing the state of the security function with management. Showing executives that you recognize the elements of a strong program and that you are working toward them proves you are engaged in not only good security, but good business program management.

If you'd like to take your own free Security Universe Assessment, contact us.

Visit the Security Executive Council web site to view more resources in the Security Program Strategy & Operations > Strategic Planning/Management series.

About the Security Executive Council

The SEC is the leading research and advisory firm focused on corporate security risk mitigation solutions. Having worked with hundreds of companies and organizations we have witnessed the proven practices that produce the most positive transformation. Our subject matter experts have deep expertise in all aspects of security risk mitigation strategy; they collaborate with security leaders to transform security programs into more capable and valued centers of excellence. Watch our 3-minute video to learn more**.**

Contact us at: contact@secleader.com
Website: https://www.securityexecutivecouncil.com/