Elements of Cybersecurity Roles

Va — Vulnerability assessment

Cy — Understand cyber risk by business unit, site, risk owner

Ld — Set and lead technology strategy

Id — Identify and report CVEs

Tl — Map and monitor threat landscape

Es — Establish infosec vision

Ri — Understand risk appetite of the board

As — Assign risk owners, and set goals

Ap — Get board buy-in and approval

Cb — Prioritize cyber risk and accept certain risk items

Sp — Sponsor cybersecurity initiatives

Pr — Prioritize vulnerabilities

Sc — Evaluate security control effectiveness

Cm — Ensure organization is compliant

Bu — Set budgets, and estimate costs

Re — Report on cybersecurity effectiveness

Cr — Create and execute operational plan

Tr — Demonstrate risk trending over time

Dm — Report on risk reduction over time

Pa — Manage patching activities

De — Deploy SIEMs and other SOC tools

In — Discover and analyze asset inventory

Ca — Categorize assets by subnet, location, etc.

Dt — Get full details on each asset

Re — Understand relationships b/w assets and users incl. admins

Bc — Understand business criticality for each asset

Pt — Improve relationships with Infosec partners

Co — Collaborate with IT, Dev, and SOC teams

Al — Prioritize SOC alerts

Im — Design and implement network and computer security

Sa — Develop security architecture

Np — Identify new problem areas to be addressed

Dr — Establish disaster recovery procedures

Vn — Lead vendor selection

Legend

- Vulnerability Management
- Risk Analysis
- CISO
- Security Architecture
- Security Operations
- CIO
- IT Manager

Balbix®