Shift Left to Deliver a More Secure Digital Workplace (and Receive a Bonus Impact to Corporate Culture)

Richard Addiscott

Gartner®

Picture It …

Gartner®

A Beautiful Montage Appears …

Gartner®

Picture This …

“Our people are our greatest asset!!”

Said every CEO …

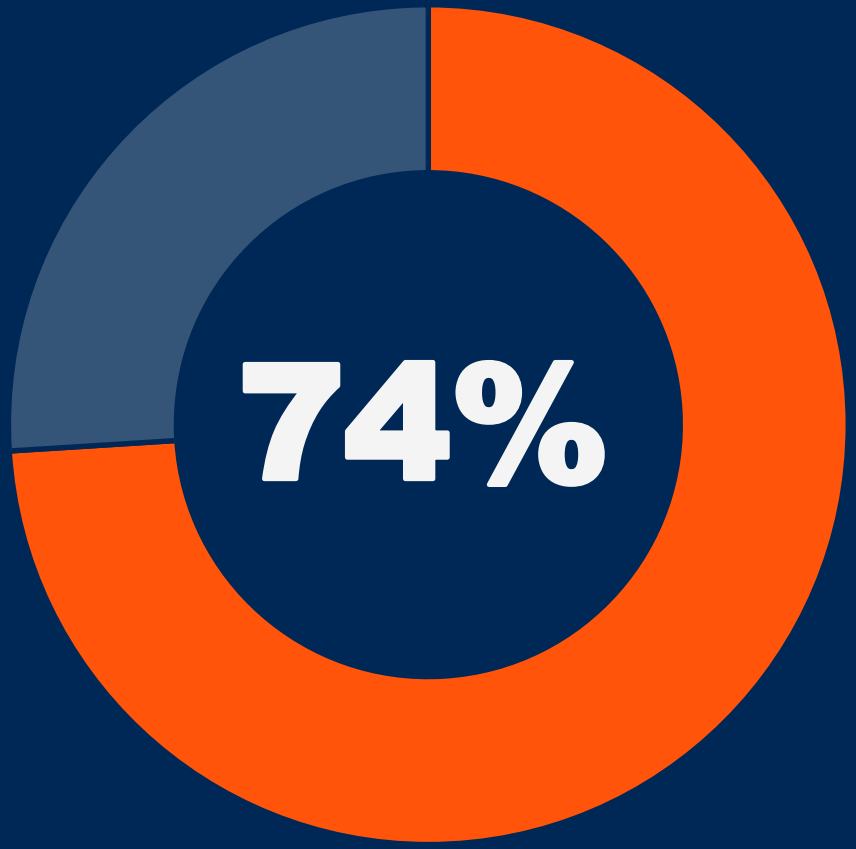
… Like ever!!!

But [a lot of] cybersecurity leaders say …

“Our end users are our weakest link …”

Gartner®

What the Research Tells Us ...



Of all data breaches involved the **human element.**

Source: 2023 Data Breach Investigations Report (DBIR), Verizon.

Gartner®

Top Breach Patterns

System Intrusion

Basic Web Application Attacks

Social Engineering

Miscellaneous Errors

Source: 2023 Data Breach Investigations Report (DBIR), Verizon.

Gartner®

Because …

Most errors that lead to a data breach were committed by …

Developers

System Admins

Source: 2023 Data Breach Investigations Report (DBIR), Verizon.

Gartner®

“Our end users are our weakest link…”

Gartner®

Traditional Security Awareness Efforts

Your Employees Have Been The Primary Focus

Gartner®

Traditional Security Awareness Efforts

Internal Digital Supply Chain

Gartner®

Traditional Security Awareness Efforts

Digital Initiative Conceived

Digital Initiative Design Phase

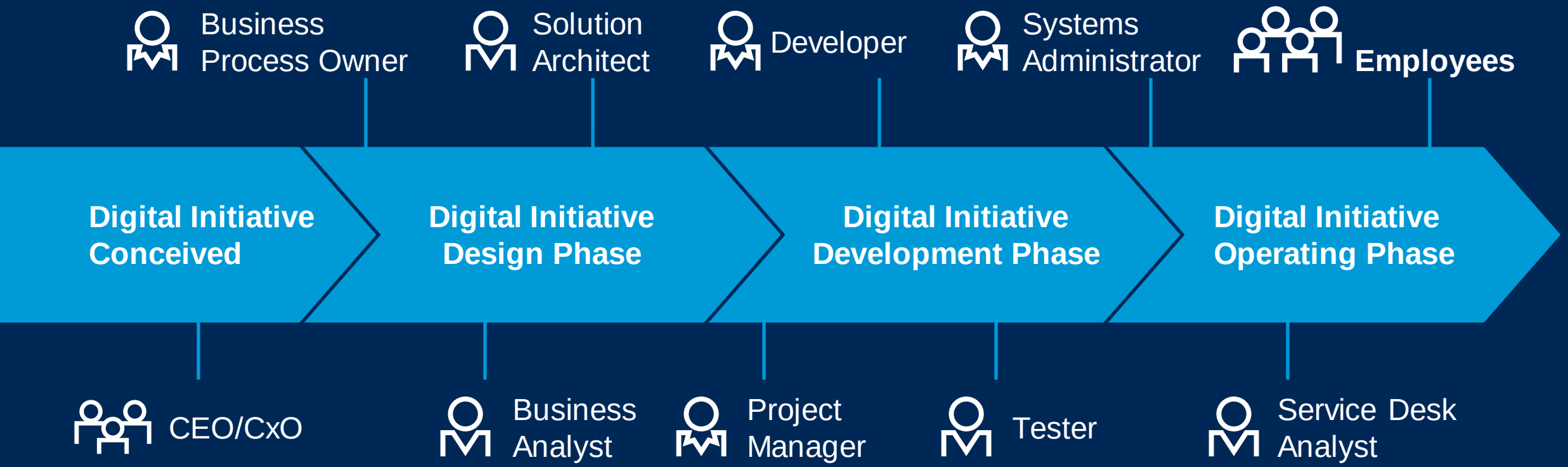
Digital Initiative Development Phase

Digital Initiative Operating Phase

Internal Digital Supply Chain

Gartner®

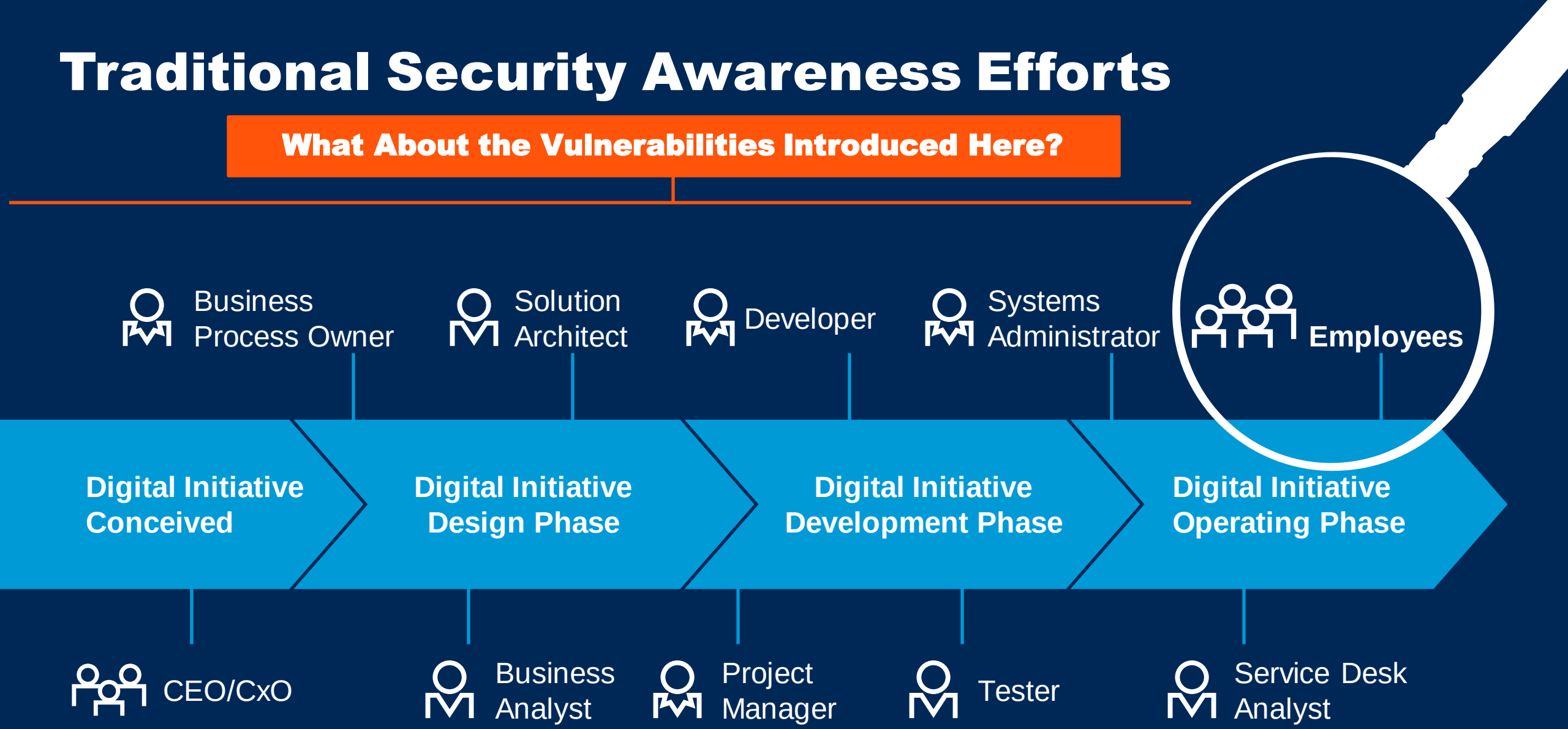
Traditional Security Awareness Efforts



Gartner®

Traditional Security Awareness Efforts

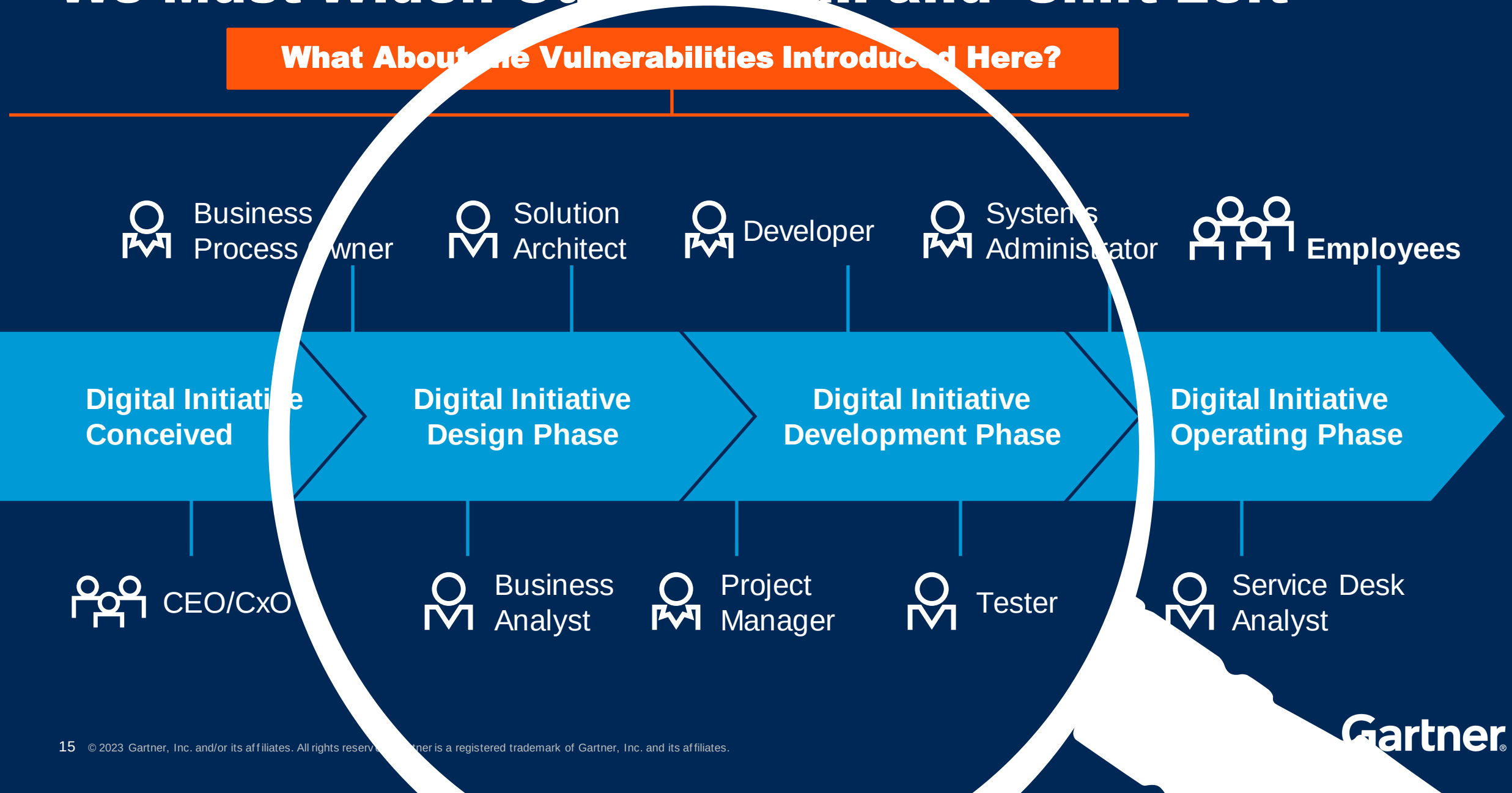
What About the Vulnerabilities Introduced Here?



Gartner®

We Must Widen Our Focus … and ‘Shift Left’

What About the Vulnerabilities Introduced Here?



Gartner®

You will optimize your opportunities to secure your digital workplace by 'shifting left' and widening your behavior and culture change efforts ...

Gartner®

Security Behavior and Culture Program — SBCP

Gartner®

The Gartner PIPE Framework

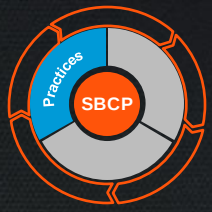
Gartner®

SBCP and the Gartner PIPE Framework

A SBCP focuses on **fostering new ways of thinking** and **embedding new behavior** with the intent to **provoke** new, more **secure ways of working** across the organization.

Gartner®

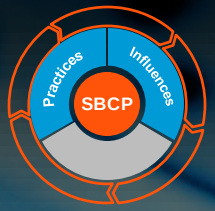
Practices — It's More Than Just CBT



- Learning and Development
- Threat Simulation
- UX Design
- Marketing and Communications/PR
- Security Coaching
- Security Champions Programs
- Organizational Change Management
- Human-Centered Security Design
- Culture Hacking/Hacks
- Data Analytics
- Nudge Theory
- Insider Risk Management

Gartner®

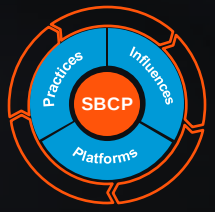
Influences — It's More Than Just Roles and Responsibilities …



- Executive Support Levels
- Approved Budget
- Organization Structure & Demographics
- Existing Cultural Values and Norms
- Behavior Gap (Current vs. Desired)
- Enterprise Strategic Objectives
- Threat and Risk Environment
- Governance Structures
- Regulatory Landscape
- Levels of Access
- Cyber/Digital Literacy Levels
- Digital Connectedness
- Communication Style
- Industry Sector

Gartner®

Platforms — Point Solutions Won't Deliver



- Learning Delivery/CBT
- Threat Simulation
- Security Monitoring
- User Behavior Analysis
- Artificial Intelligence/ML
- Identity and Access Management
- Data Loss Prevention
- Gamification
- Data Analytics
- Communications
- Robotic Process Automation
- Integration
- SAST/DAST/IAST

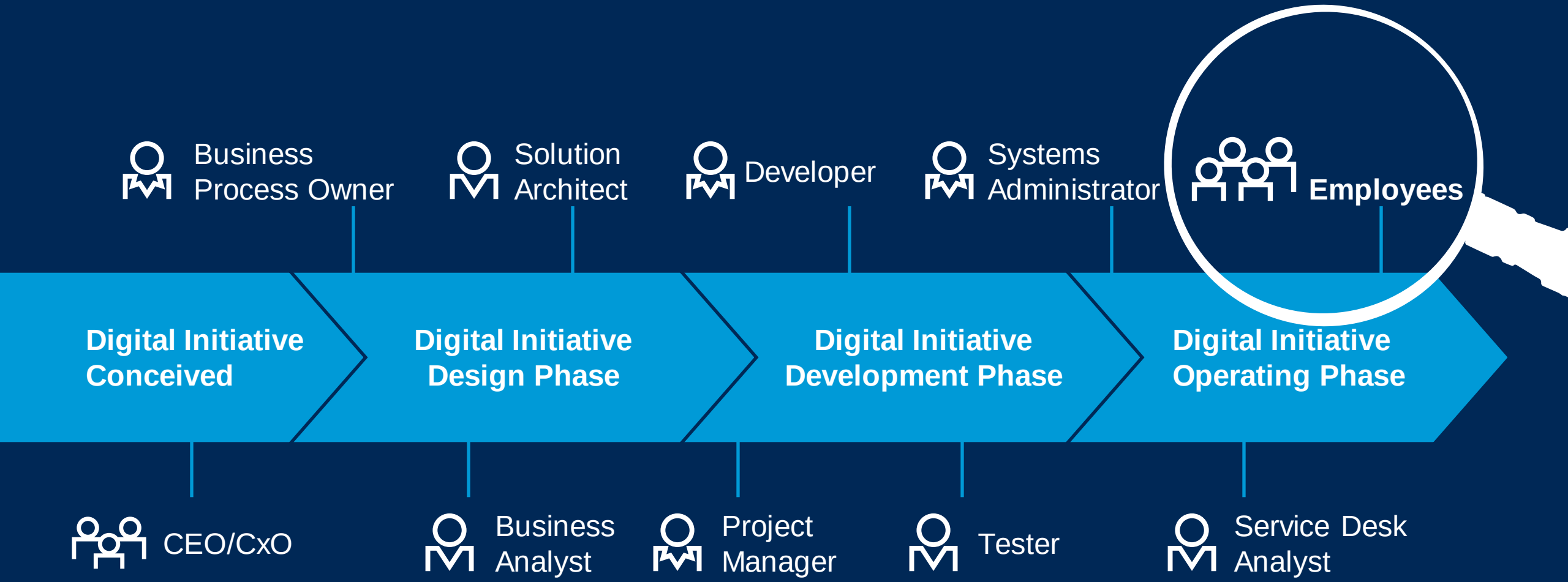
SAST = Static Application Security Testing
DAST = Dynamic Application Security Testing
IAST = Interactive Security Testing

Gartner®

Techniques to Help ‘Shift Left’ …

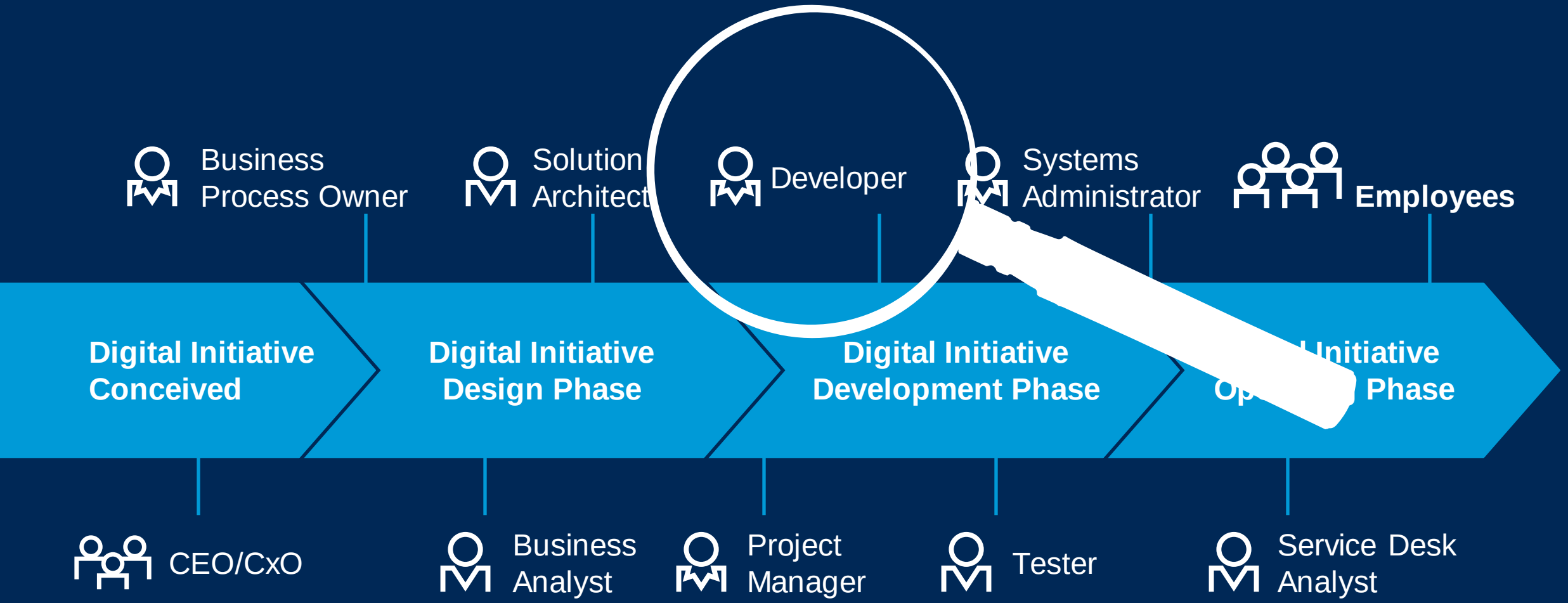
Gartner®

Shifting Left — Move From DevOps to DevSecOps



Gartner®

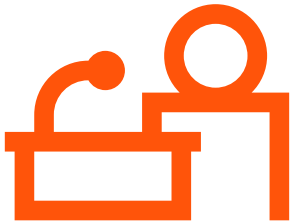
Shifting Left — Move From DevOps to DevSecOps



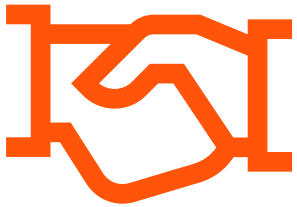
Gartner®

Establish a DevOps Security Coaching Program

Recruit qualified internal talent

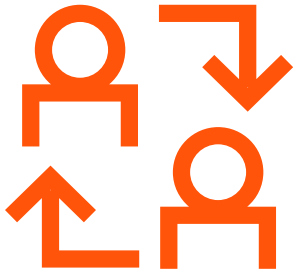


Train coaches using real-world scenarios



Connect coaches with the security team

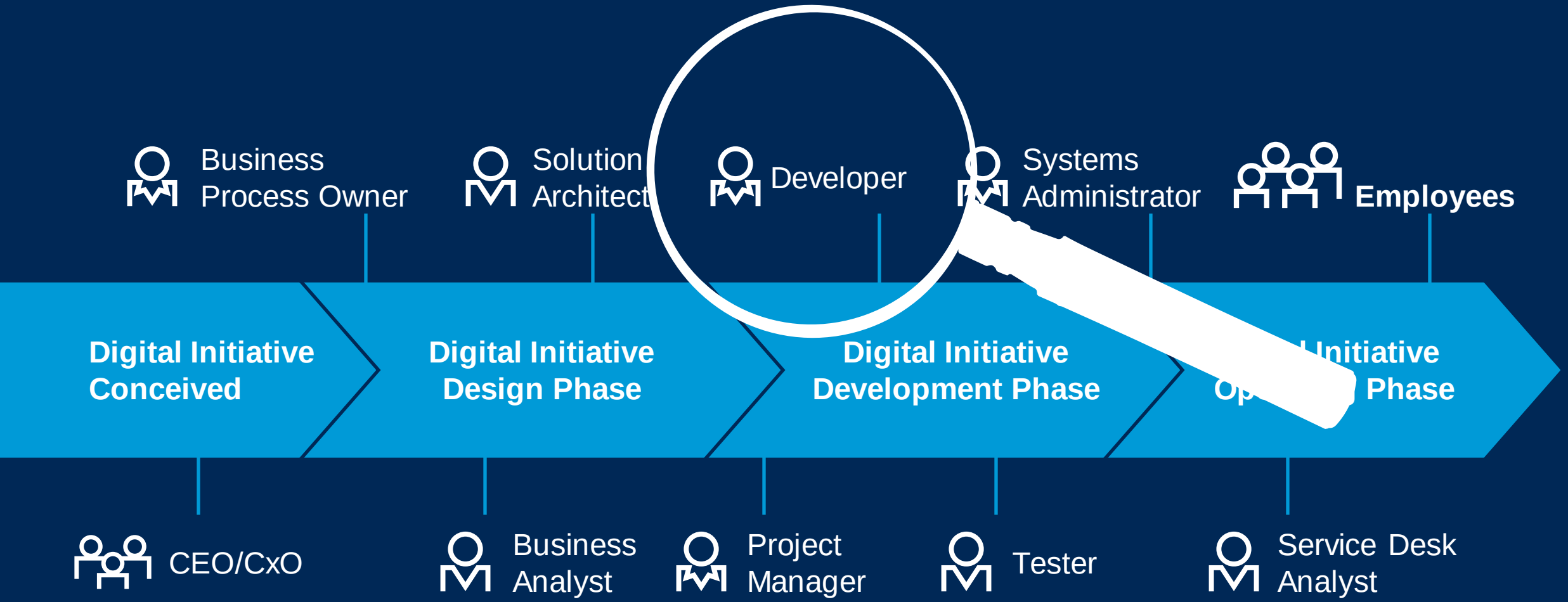
Set up a reward and recognition scheme



Foster developer, security, I&O collaboration

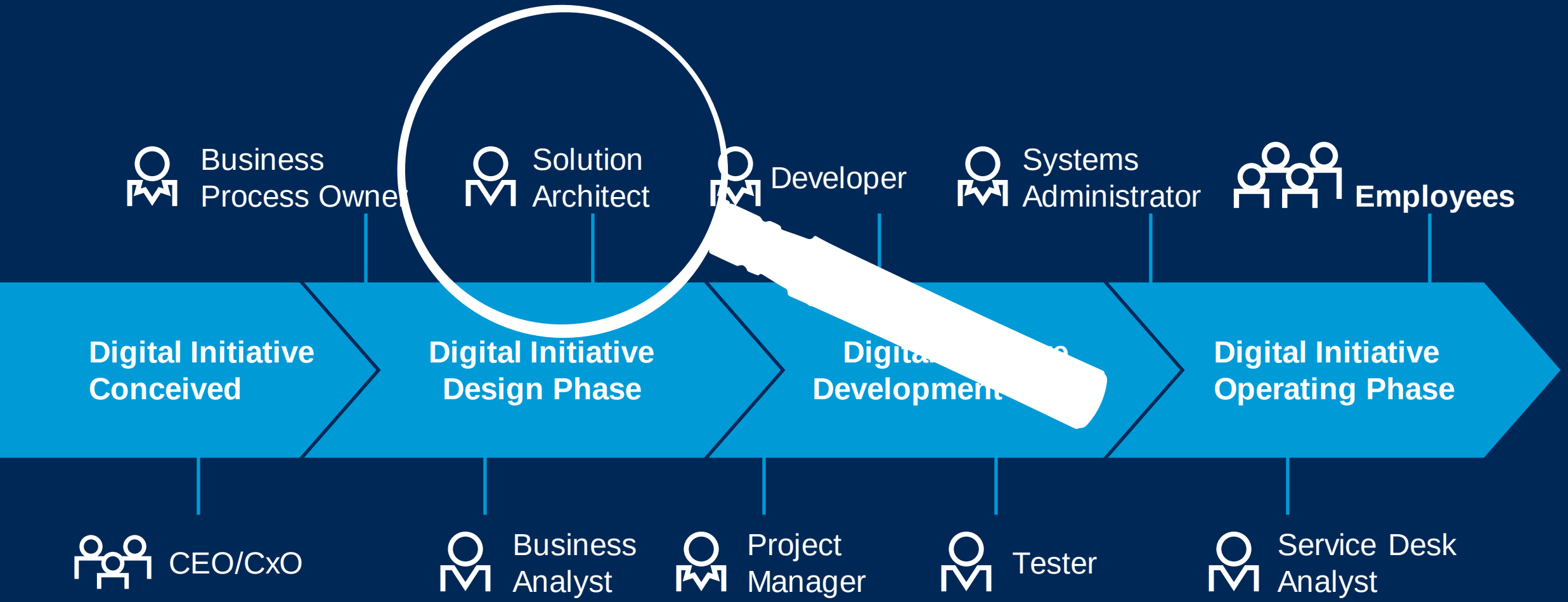
Gartner®

Shifting Left — Move From DevOps to DevSecOps



Gartner®

Shifting Left — Human-Centric Security Design



Gartner®

What Is Human-Centric Security Design?

Human-centric security design (HCSD) prioritizes the role of employee experience — rather than technical considerations alone — across the controls management life cycle.

Gartner®

What Is Human-Centric Security Design?

Human-centric security design (HCSD) prioritizes the role of employee experience — rather than technical considerations alone — across the controls management life cycle.

Gartner®

Human-Centric Security Design

Empathy-Based Engagement

Intentional Collaboration

Flexible Security Experience

Ethically-Centered

Gartner®

Human-Centric Security Design

Empathy-Based Engagement

Intentional Collaboration

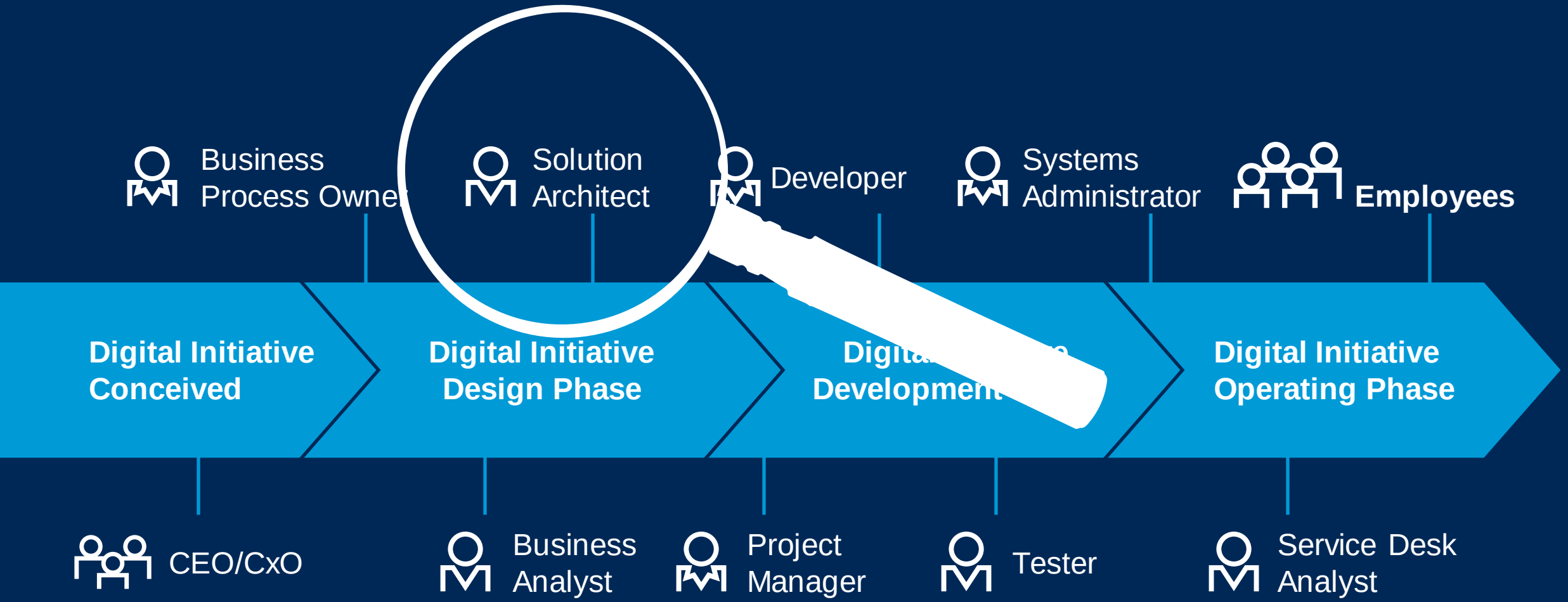
Flexible Security Experience

Ethically-Centered

- Reduced Operational Friction
- Improved Control Adoption
- Improved Control Effectiveness
- Reduced Cybersecurity Incidents
- Improved Business Value for Security

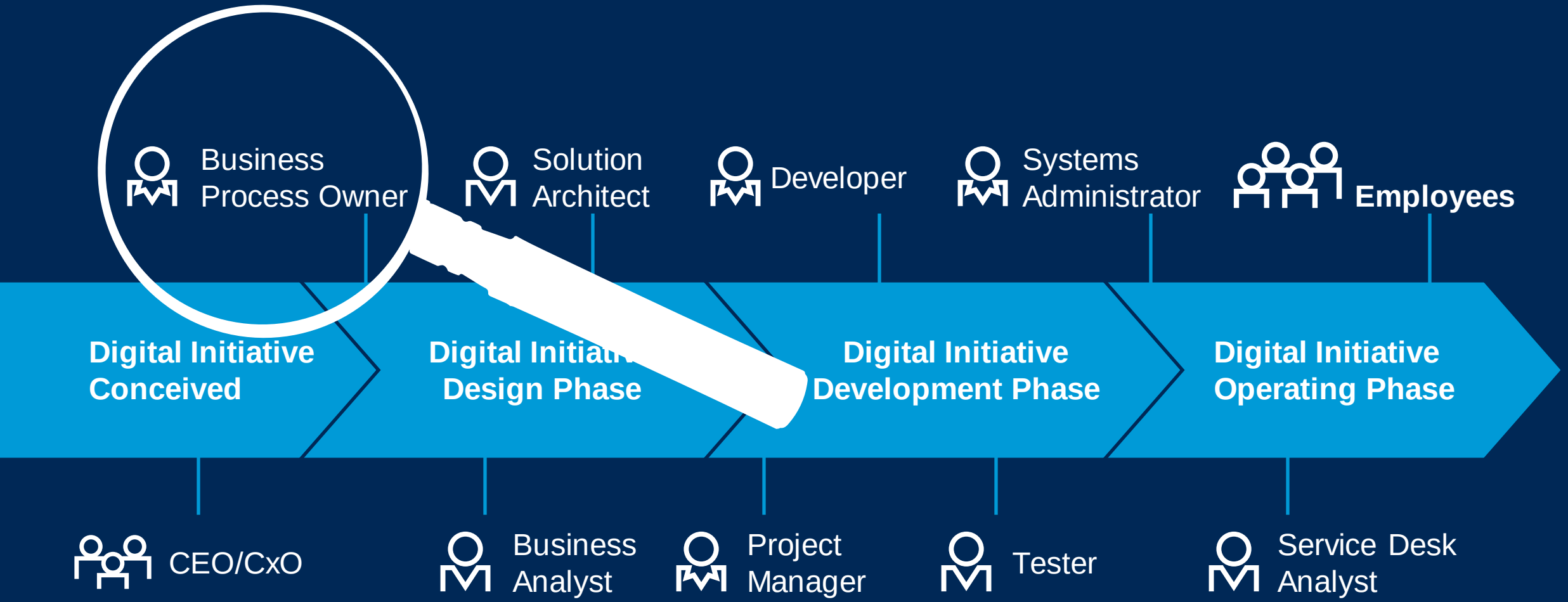
Gartner

Shifting Left — Human-Centric Security Design



Gartner®

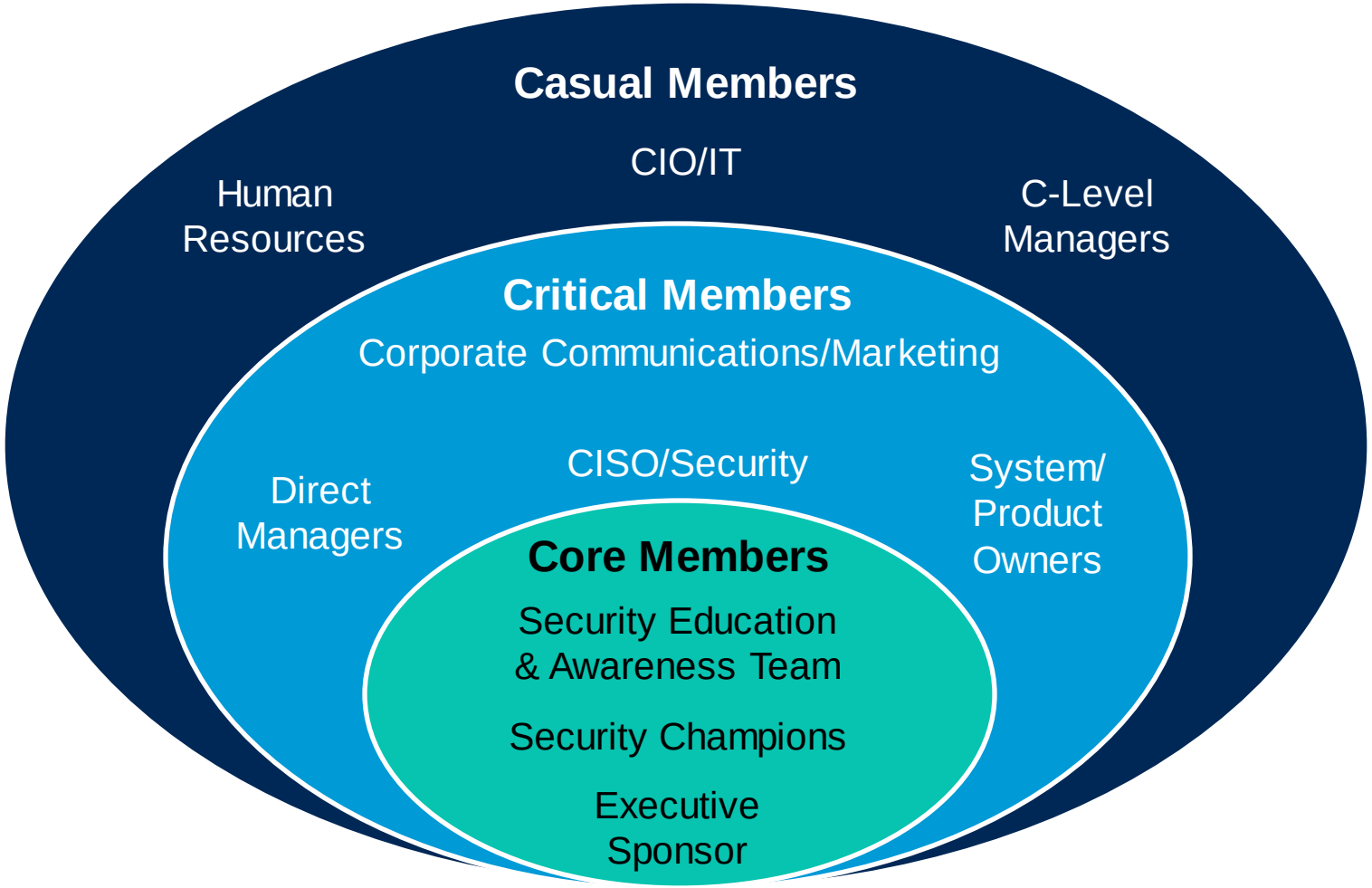
Shifting Left — Business Areas



Gartner®

Establish a Business Security Champions Program

Security Champion Program Membership Ecosystem



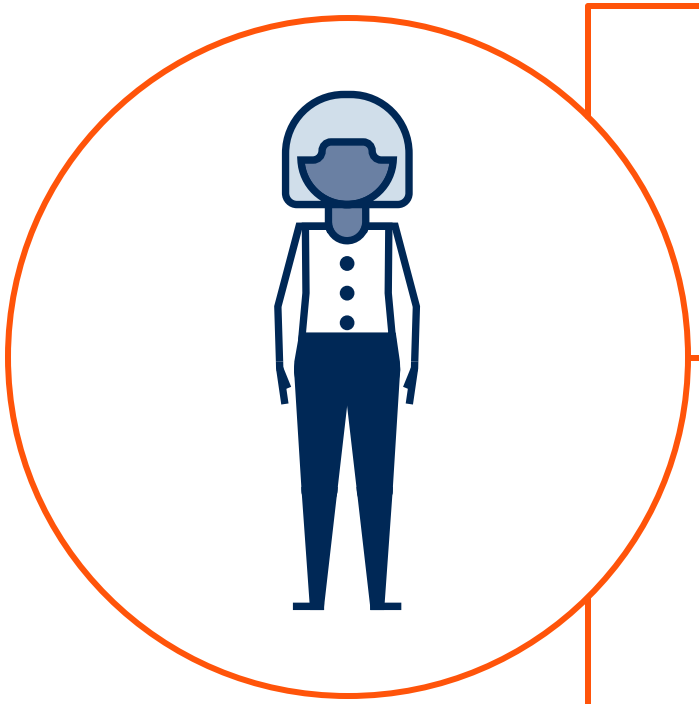
Who's Involved?

Source: Gartner

Gartner®

Establish a Business Security Champions Program

What makes a good business security champion?



Leadership Skills

- Active Listener
- Emotionally Intelligent
- Change Agent
- Problem Solver

Business Skills

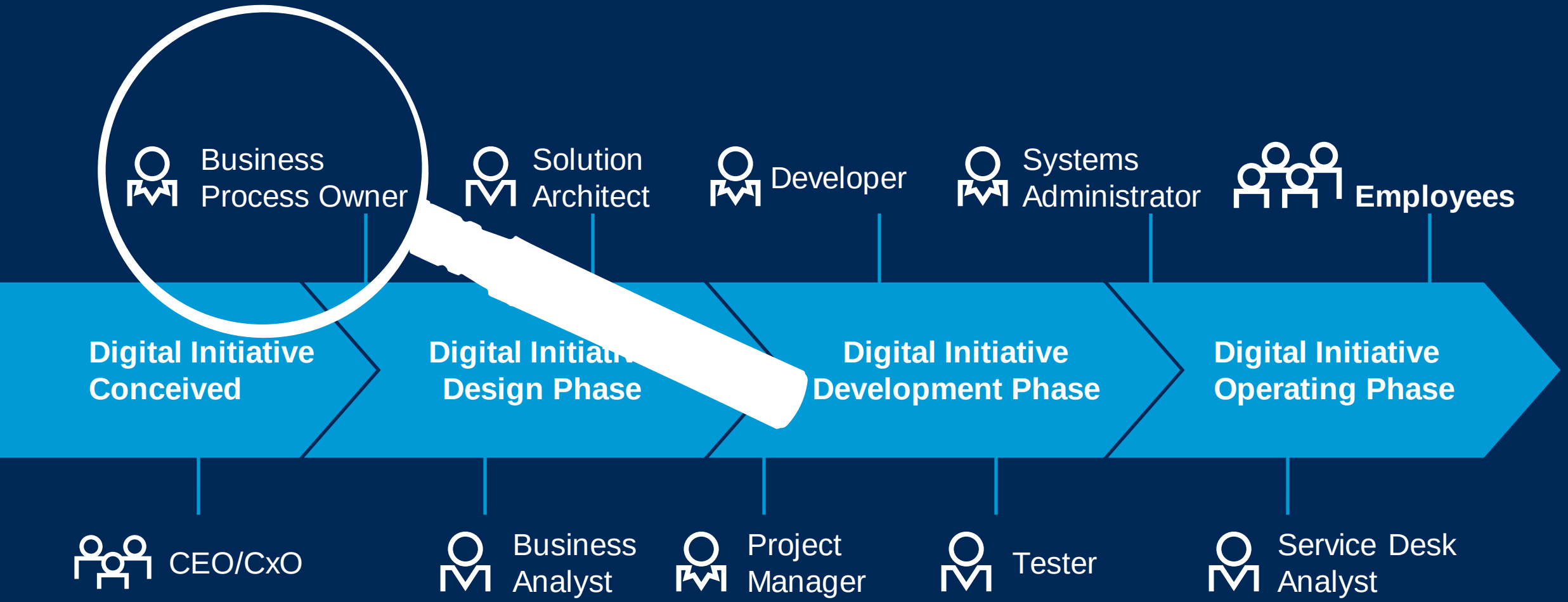
- Domain Expert
- Results Oriented
- Organizationally Aware
- Excellent Communicator

Desirable Attributes

- Interested in Security
- Learning Agility
- Organized and Proactive
- Proactive Collaborator

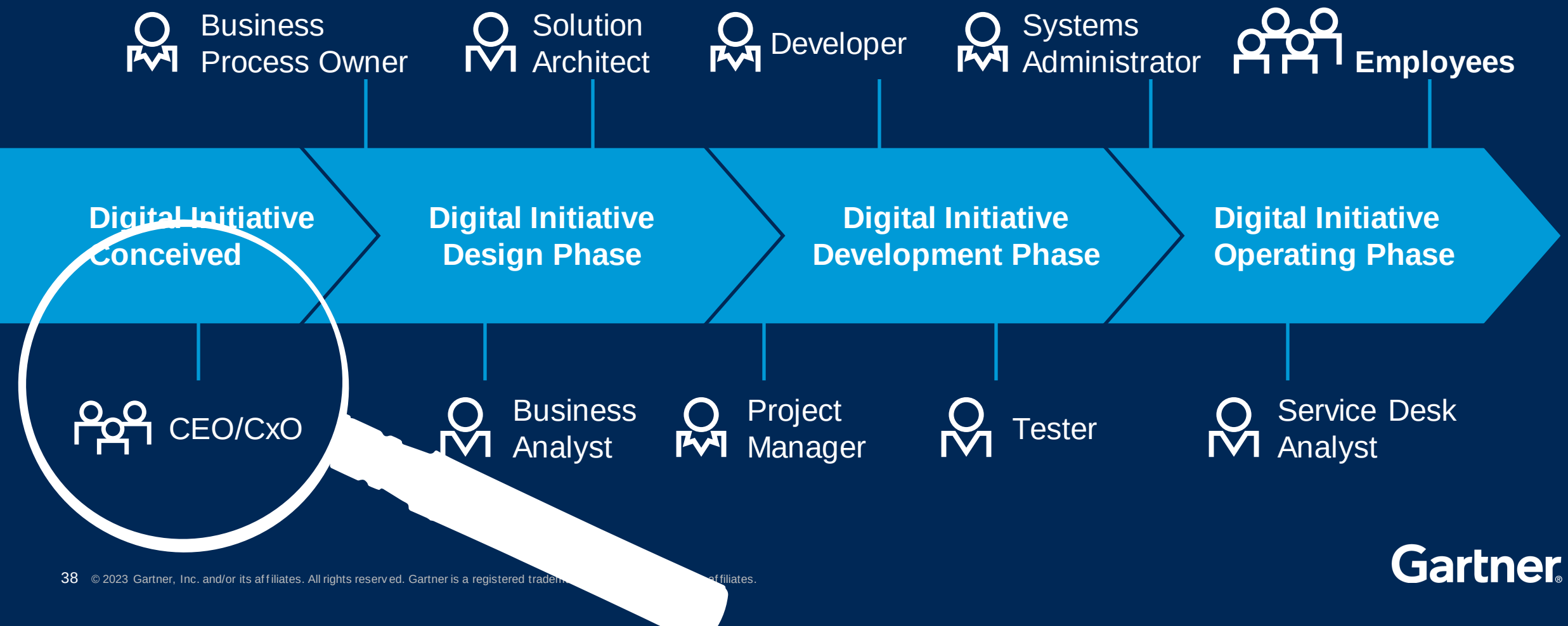
Gartner

Shifting Left — Business Areas



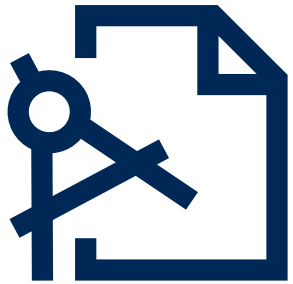
Gartner®

Shifting Left — The C-Suite

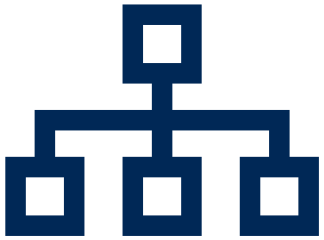


Gartner®

Governance Is Critical… the Buck for Cyber Risk Must Stop With the Right People



Set Clear Owner Accountability via an Enterprise Security Charter



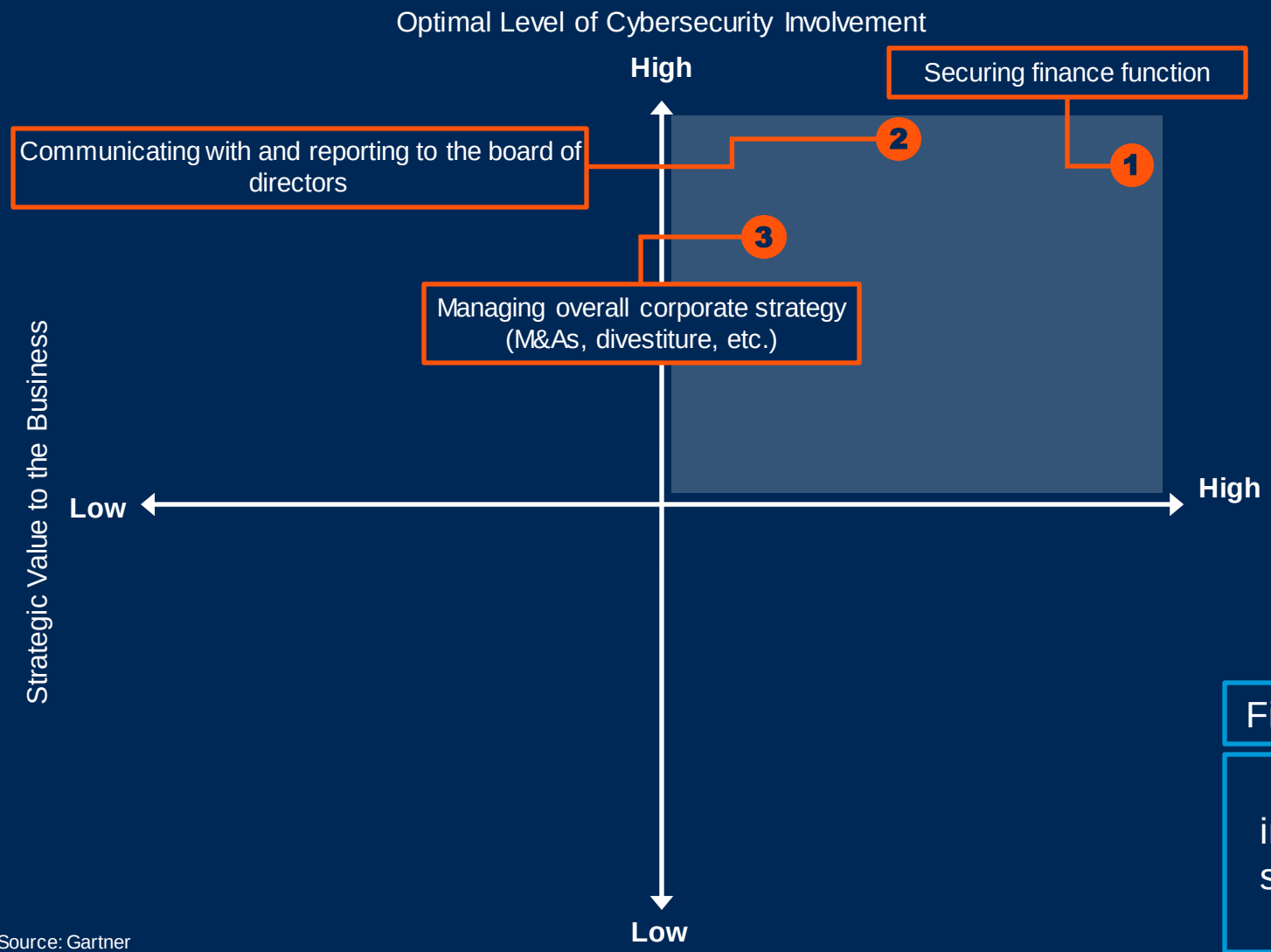
Define Cybersecurity Roles and Responsibilities via a RASCI Matrix

Build Cyber-Risk Management Into Executive JDs and Performance Management Frameworks

Gartner®

Find Your Common Ground With the C-Suite

Chart: Strategic Value & Cybersecurity Involvement in Shared Priorities



Possible CFO Priorities to Chart

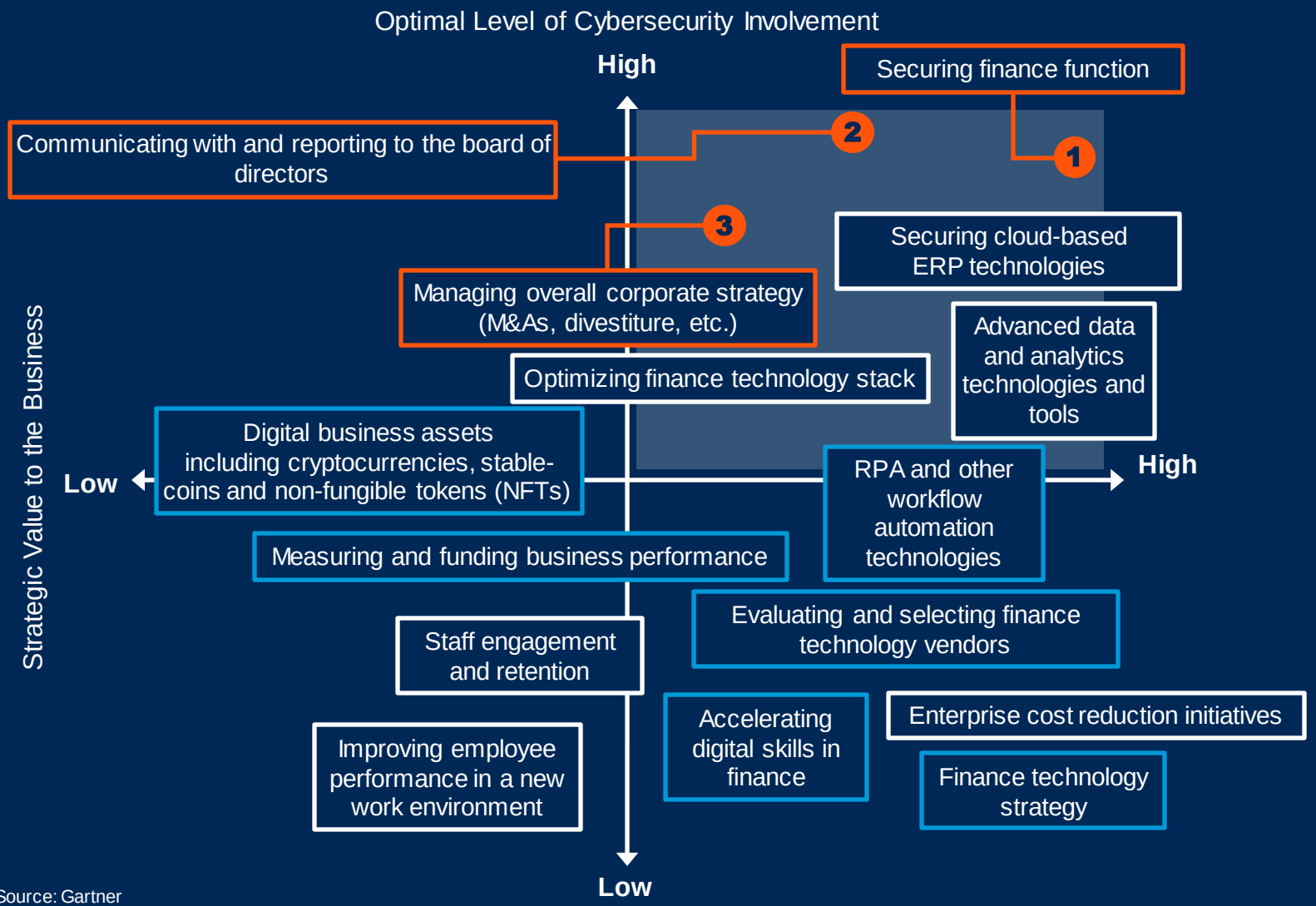
- Advanced data and analytics technologies and tools
- RPA and other workflow automation technologies
- Staff engagement & retention
- Accelerating digital skills in finance
- Securing cloud-based ERP technologies
- Measuring and funding business performance
- Enterprise cost reduction initiatives
- Improving employee performance in a new work environment
- Optimizing finance technology stack
- Finance technology strategy
- Digital business assets including cryptocurrencies, stable-coins & non-fungible tokens (NFTs)
- Evaluating and selecting finance technology vendors

Source: Gartner

Gartner®

Find Your Common Ground With the C-Suite

Chart: Strategic Value & Cybersecurity Involvement in Shared Priorities



Possible CFO Priorities to Chart

Source: Gartner

Gartner®

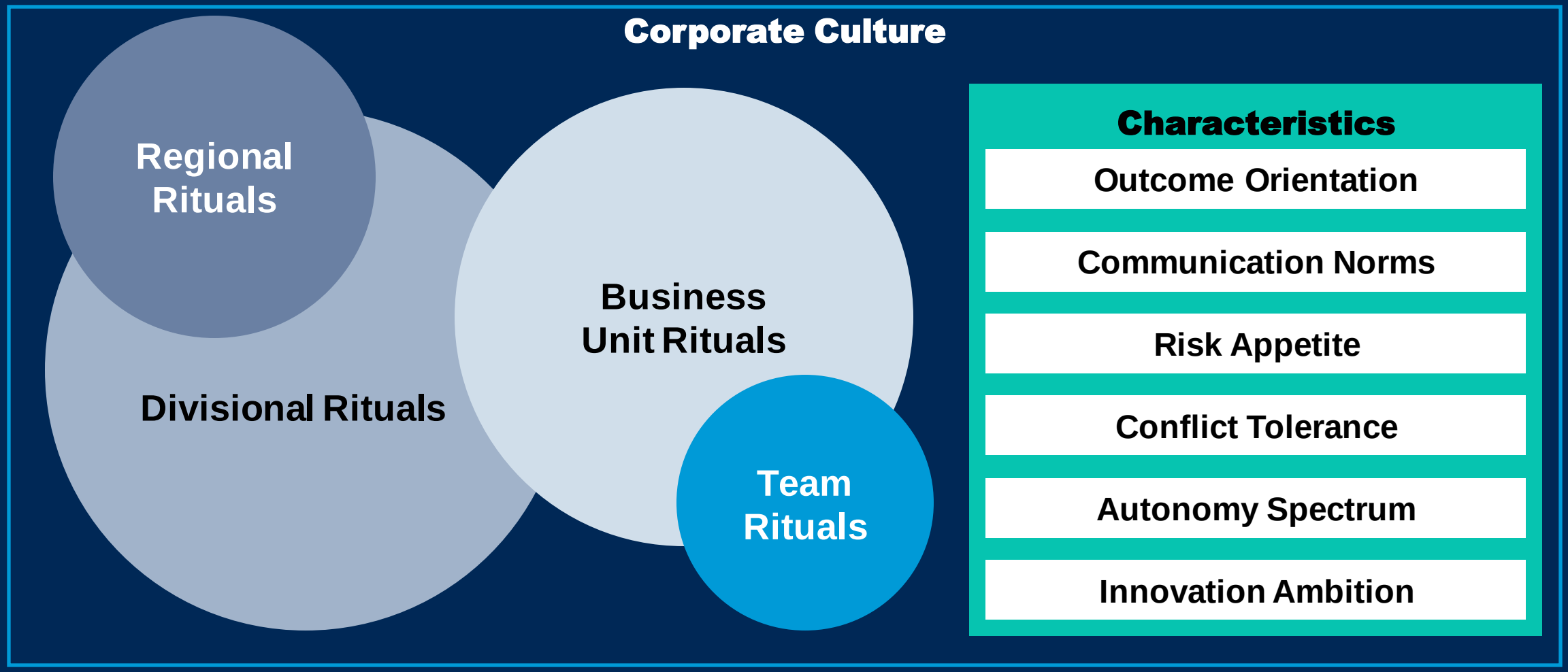
Recommendations

- Extend your security program beyond just raising employees ‘awareness’ and change your mindset about them being the weakest link.
- Establish a security coaching program in your DevOps teams and extend the reach and penetration of your security-related messaging through a business security champions program.
- Take a human-centric approach to security control design to help improve employee control adoption.
- Formalize and enforce cyber-risk management accountability in job descriptions and look for common goals with the C-Suite to help improve executive buy-in on cybersecurity objectives.

Benefits to Corporate Culture ...

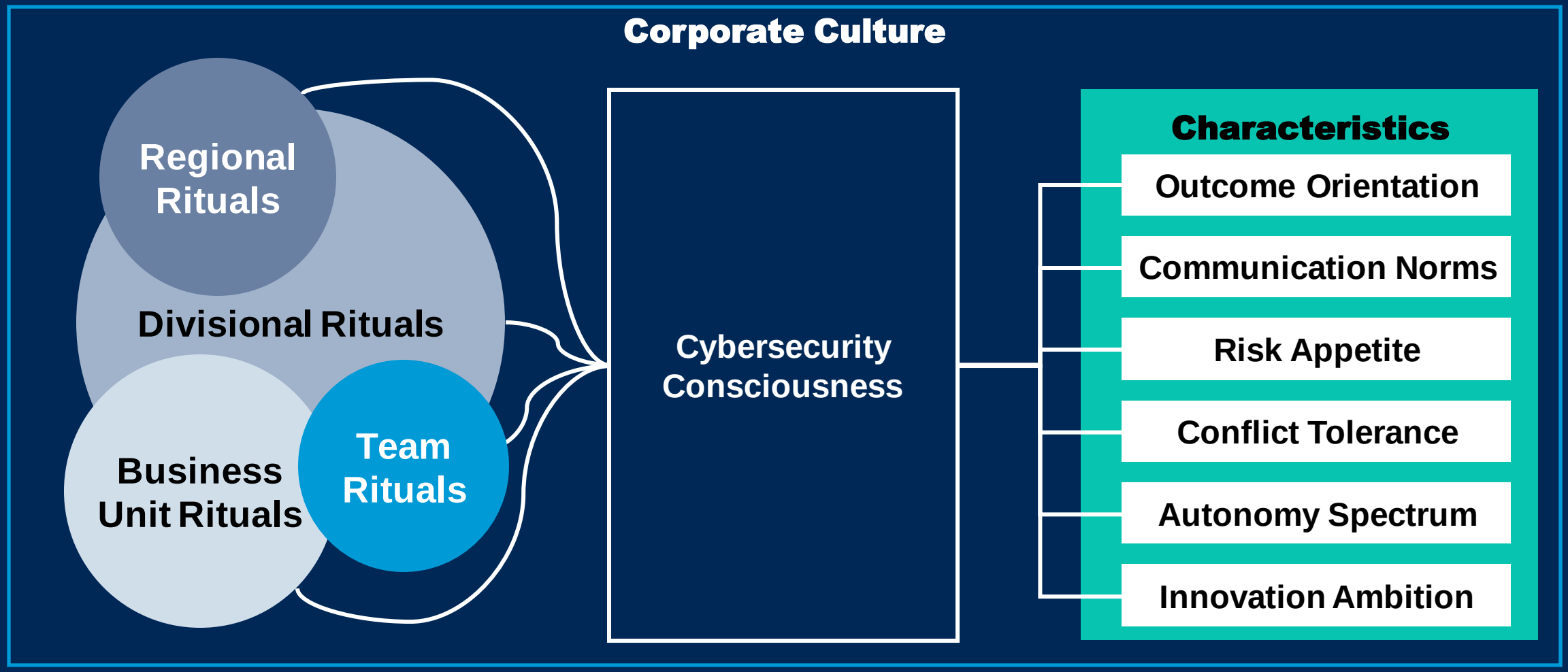
Gartner®

Anatomy of a Corporate Culture



Gartner®

Shifting Left Improves the Cybersecurity Consciousness of the Corporate Culture



Gartner®

Recommended Gartner Research

- **CISO Foundations: Build a Culture of Security Consciousness: Introducing the Gartner PIPE Framework**
  Richard Addiscott, Andrew Walls, William Candrick and Christine Lee
- **3 Essential Steps to Enable Security in DevOps**
  Daniel Betts, Manjunath Bhat, Hassan Ennaciri and Chris Saunderson
- **Top Trends in Cybersecurity 2023**
  Richard Addiscott, Alex Michaels, Jeremy D'Hoinne and Others
- **Tool: A CISO's Guide for Conversations With the CFO**
  Cybersecurity Research Team
- **Ignition Guide to Designing and Launching a Security Champion Program**
  Cybersecurity Research Team

Gartner®

Recommended Gartner Research

- **Establish a Security-Conscious Culture Using Behavioral Economics**
  Tom Scholtz
- **Predicts 2023: Cybersecurity Industry Focuses on the Human Deal**
  Tom Scholtz
- **Tool: A CISO's Guide for Conversations With the CMO**
  Cybersecurity Research Team
- **Tool: A CISO's Guide for Conversations With the Chief Sales Officer**
  Cybersecurity Research Team
- **Tool: Driving Secure Employee Behaviors**
  Cybersecurity Research Team

Gartner®