Conf: 42 Golang

June 24, 2021

Stone Creek
COACHING

Gordon Rudd

Chief Vision Officer
Stone Creek Coaching
+1 (918) 640-5706
Gordon@stonecreekcoaching.com

Gordon founded Stone Creek Coaching after coaching CISOs, CTOs, & CIOs for the last 15 years.

He loves to give back to the technical community, he's been so fortunate to be a part of for over 40 years, by helping technical people discover their potential to become technical leaders.

Gordon's career includes programming, systems engineering, network engineering, enterprise information architecture, project management, information security, vendor management, risk management, and process improvement.

Specializing in cybersecurity, high-performance teaming, and coaching C-Level personnel and the organizations they serve.

He is frequently asked to speak at industry events on cybersecurity, IT operations management and organizational behavior. Gordon has a BBA in Finance from the University of Oklahoma and an MBA from West Texas A&M University.

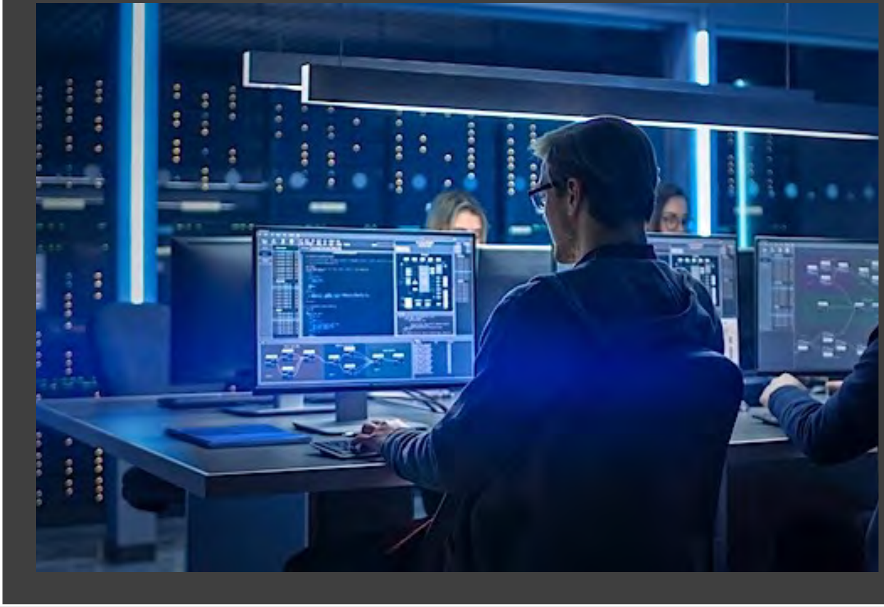
Every CISO’s First 90 days

Achieving Lasting Success as CISO

Agenda

- You wanted to be a CISO?
- 30-60-90 Day Plans
- You’re a CISO now; what should you be doing?
- Creating your MAP
- Get your head in the game
- Where to next?

DREAM JOB



C
I
S
O
CHIEF
INFORMATION
SECURITY
OFFICER

This is a Rockstar

Credit: newsweek.com

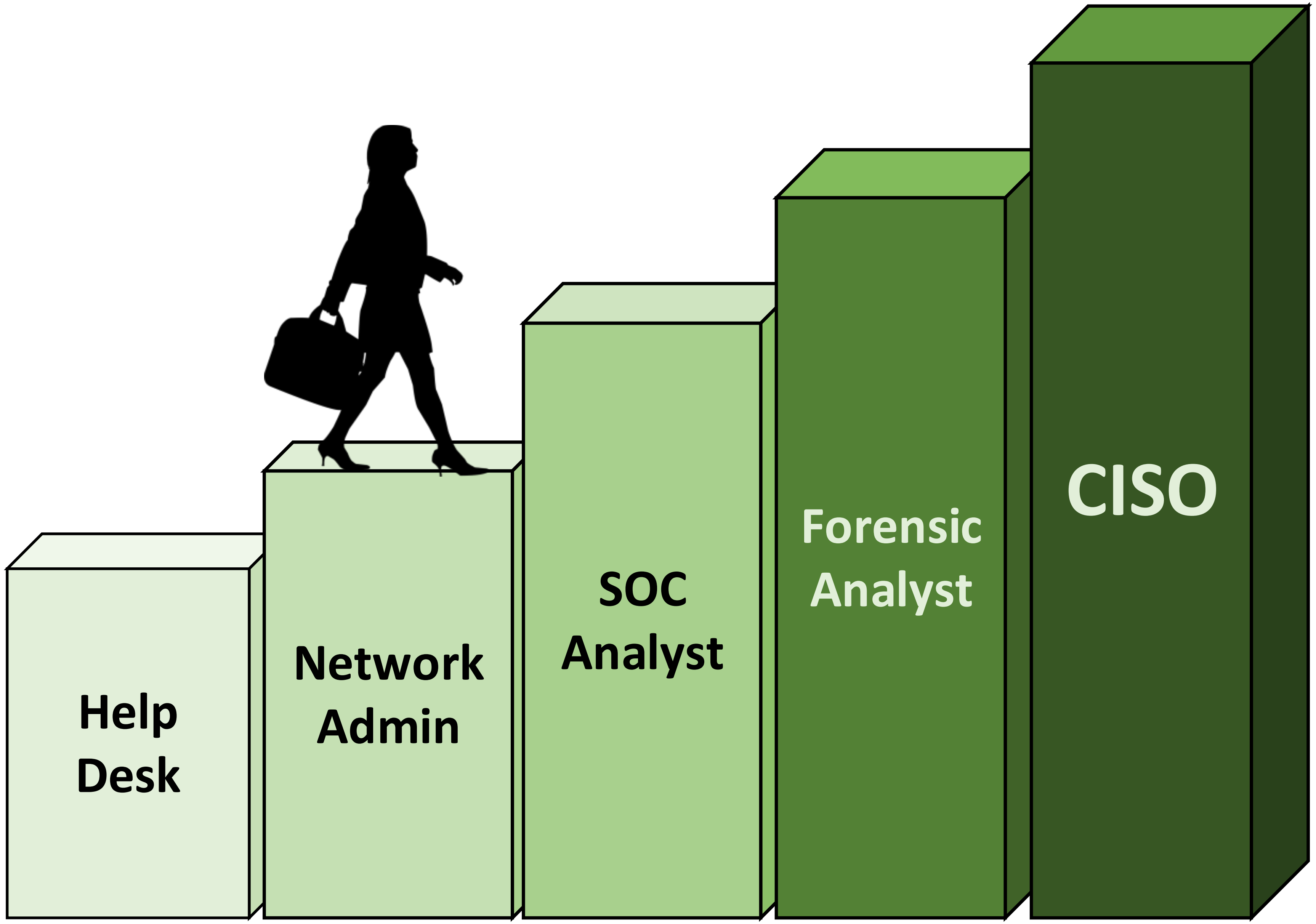
This is a CISO

Credit: gettyimages

MAP

Measure • Assess • Plan

- Measure what’s in place
- Assess the gap - what’s needed
- Plan the work – work the plan



Help Desk

Network Admin

SOC Analyst

Forensic Analyst

CISO

Nirvana for a CISO hinges on 9 skills

1. The tone from the top
2. Governance | Risk | Compliance
3. The KISS principle
4. Employee ownership
5. Solving problems - not buying new tech
6. Finding your company rhythm
7. Due diligence
8. Collaboration
9. Automating everything (as possible)

What type of CISO are you?

Technical vs. Managerial | Hands-On vs. Executive

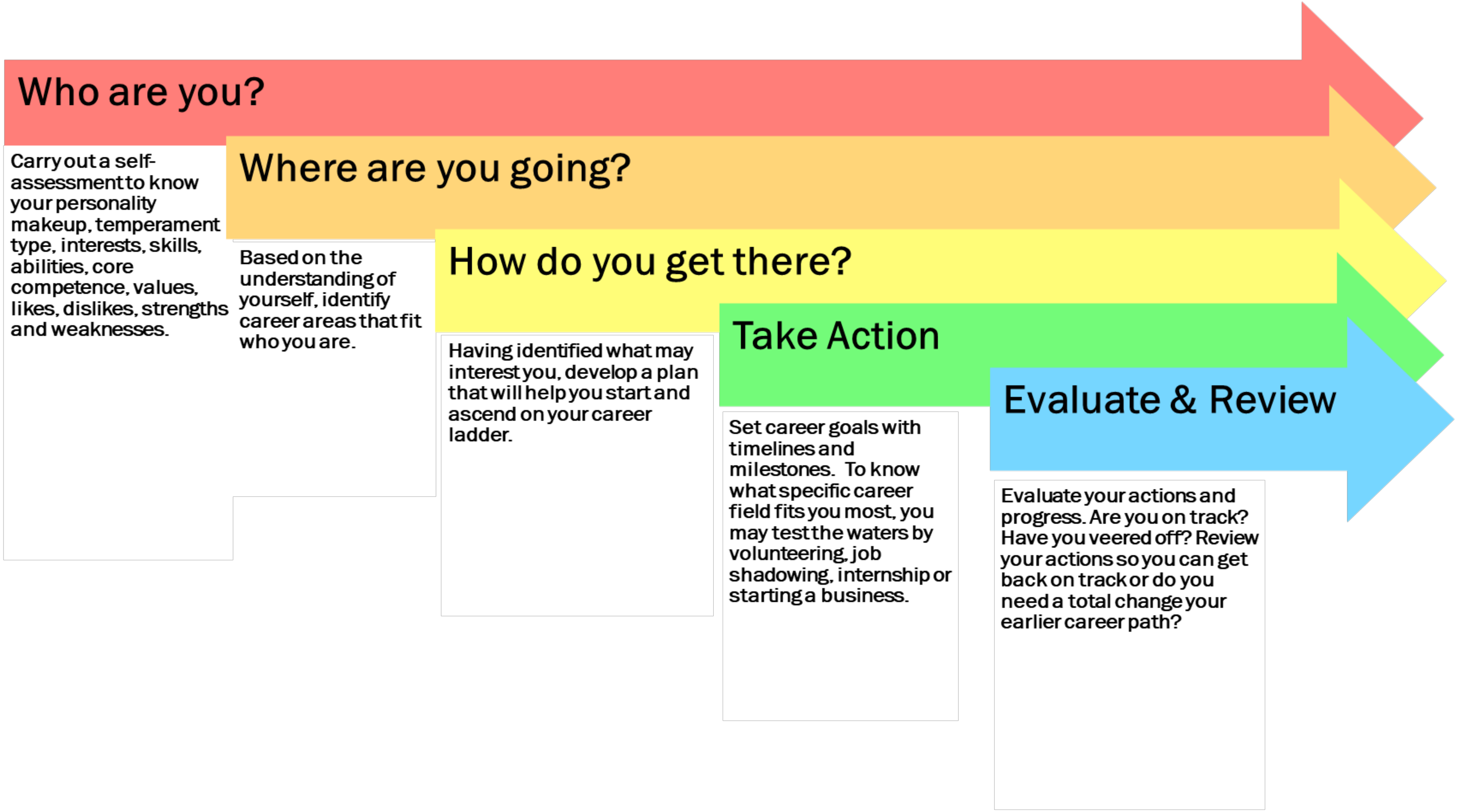
- Technical-oriented CISO (aka TISO)
- Policy-oriented CISO (aka BISO)
- Strategically-oriented CISO (aka SISO)

MAP

Measure • Assess • Plan

Yourself

- Agonizing self appraisal
- What are you?



Who are you?

Carry out a self-assessment to know your personality makeup, temperament type, interests, skills, abilities, core competence, values, likes, dislikes, strengths and weaknesses.

Where are you going?

Based on the understanding of yourself, identify career areas that fit who you are.

How do you get there?

Having identified what may interest you, develop a plan that will help you start and ascend on your career ladder.

Take Action

Set career goals with timelines and milestones. To know what specific career field fits you most, you may test the waters by volunteering, job shadowing, internship or starting a business.

Evaluate & Review

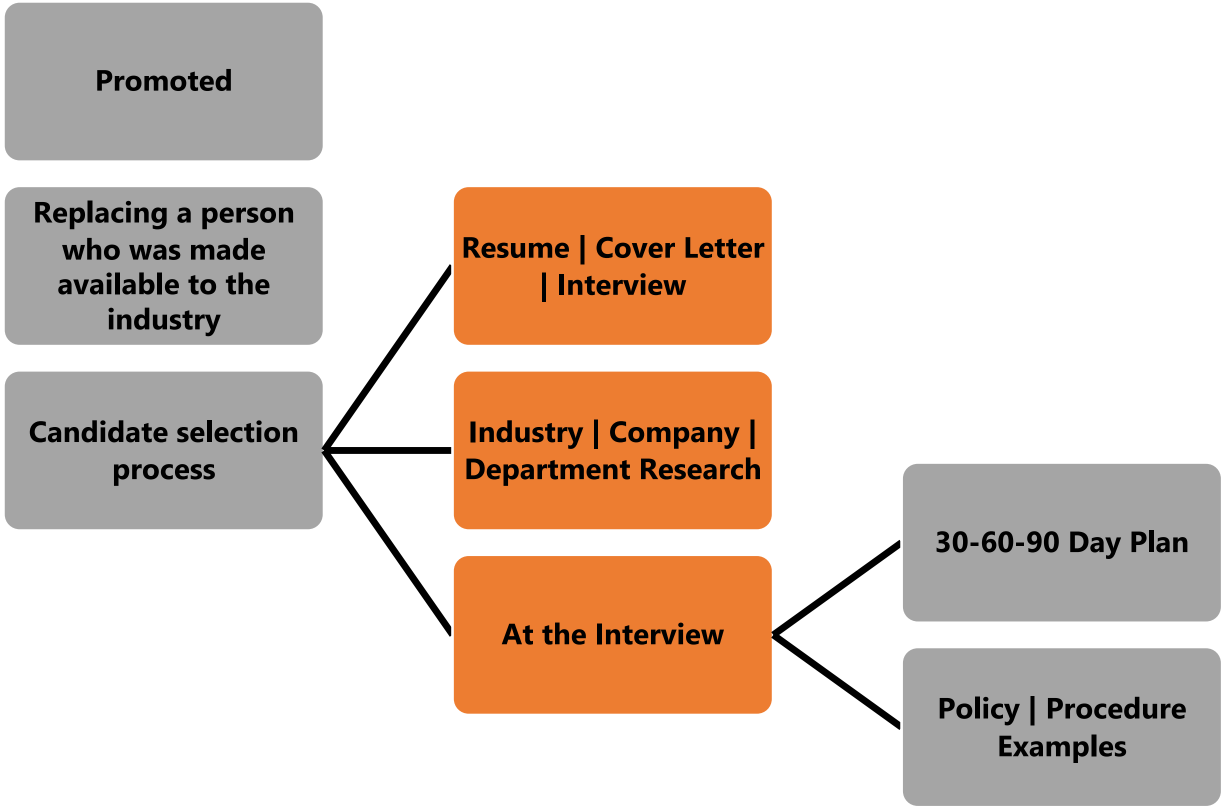
Evaluate your actions and progress. Are you on track? Have you veered off? Review your actions so you can get back on track or do you need a total change your earlier career path?

Every pro was once an amateur.

Every expert was once a beginner.

Are you ready for the race?

How did you get the job?



Promoted

Replacing a person who was made available to the industry

Candidate selection process

Resume | Cover Letter | Interview

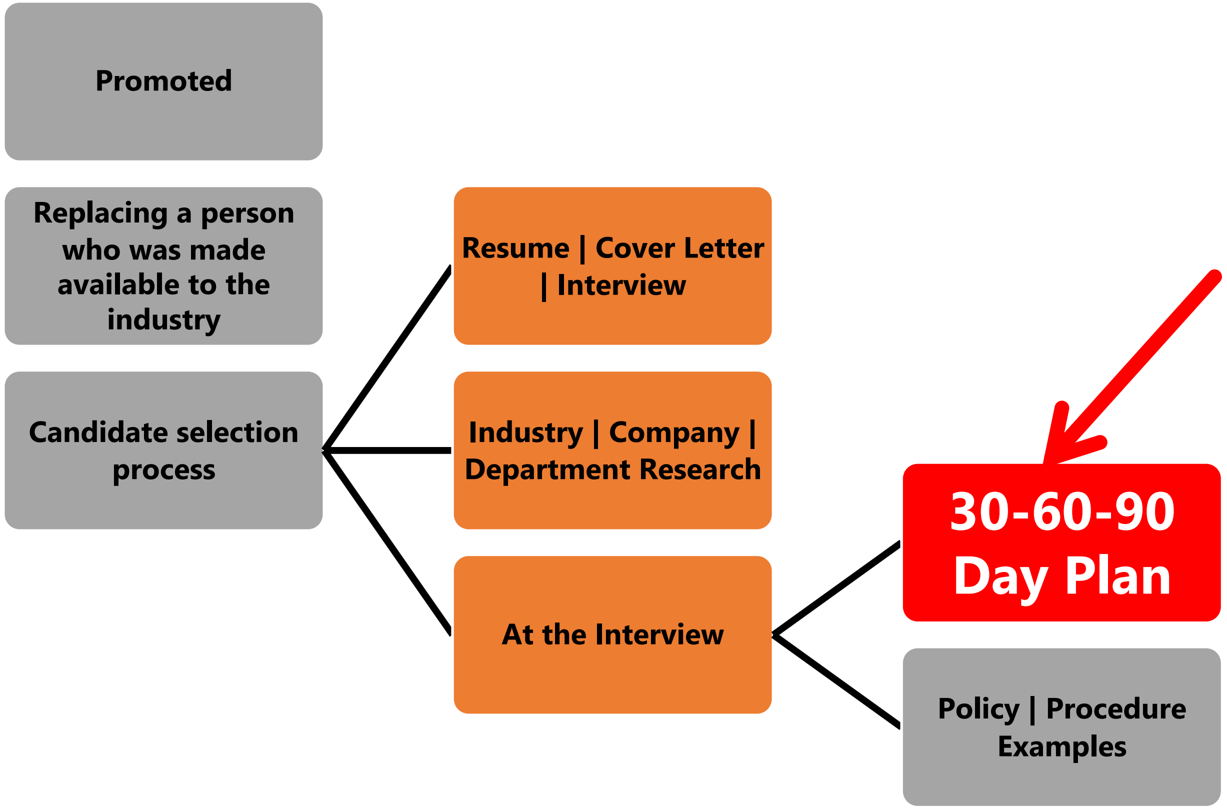
Industry | Company | Department Research

At the Interview

30-60-90 Day Plan

Policy | Procedure Examples

How did you get the job?



Promoted

Replacing a person who was made available to the industry

Candidate selection process

Resume | Cover Letter | Interview

Industry | Company | Department Research

At the Interview

30-60-90 Day Plan

Policy | Procedure Examples

Prep

- 30-60-90 day plan
- Manager's expectations
- Org chart
- Industry R&D
- Company R&D
- Department R&D

- 10 days

Measure

- Strategic & tactical plans (Policies & Procedures)
- Budget
- GRC (P&P Analysis)
- Enterprise Information Architecture
- Assets being managed
- Assets unmanaged
- Vulnerability Assessment Processes
- Personnel skill set
- Access Controls
- Interview key stakeholders
- Interview Internal Audit, external audit & Compliance

0 to 30 days

Assess

- Enterprise cybersecurity architecture vs. baseline
- Current training plan(s)
- Software development team(s)
- DevOps Team(s)
- How the organization is meeting PCI, HIPAA, CCPA, NTDFS
- Network security audit results
- Any outstanding findings from prior cybersecurity audits/exams
- Physical security
- Assess the Business Continuity Management Plan
- Assess corporate backup management strategy

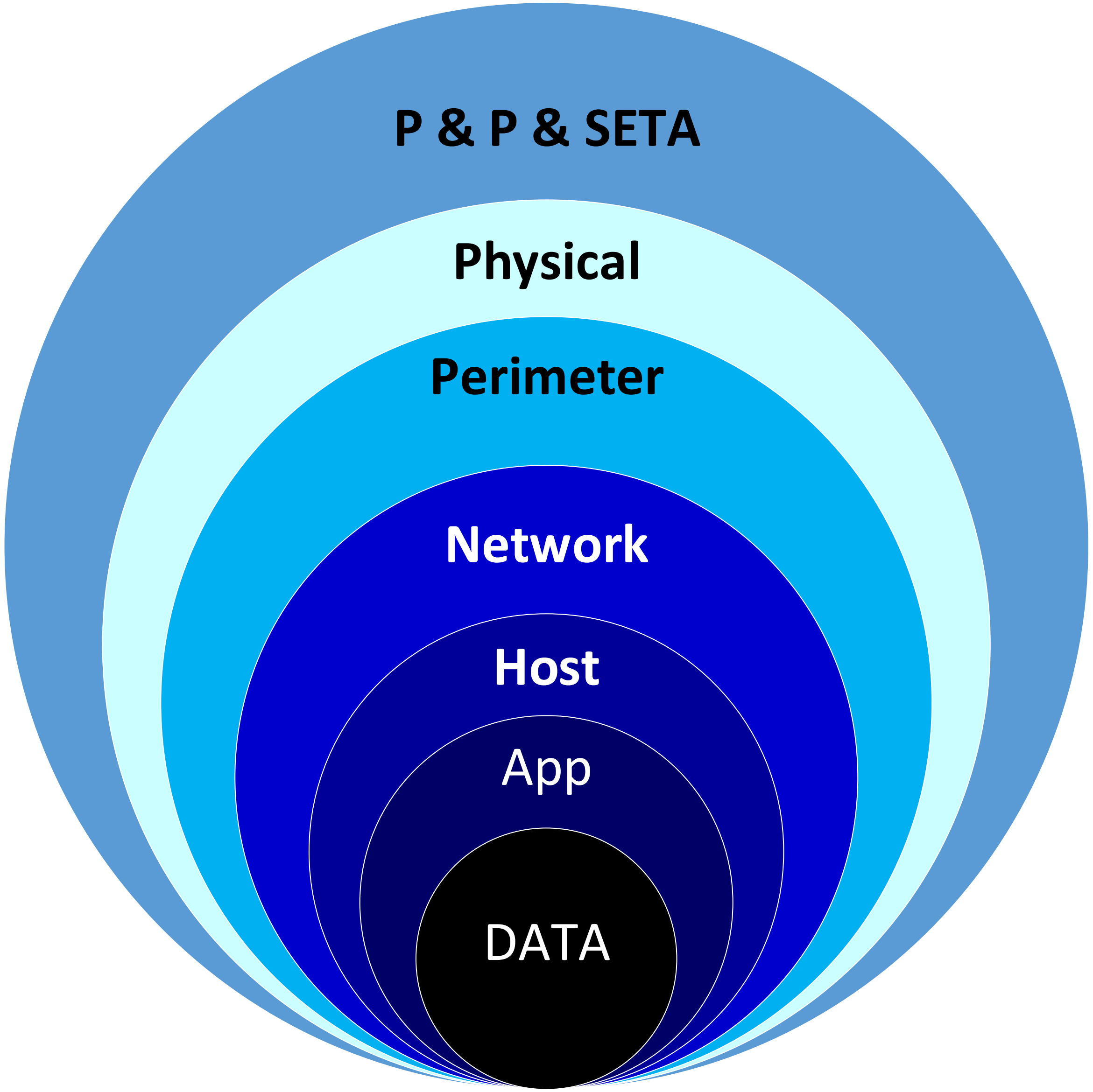
30 to 60 days

Plan

- Create Corporate Information Protection Plan
- Create Information Security Strategic Plan for the coming year
- Build you
- Social your roadmap
- Plan test of RTO, RPO, and MAD
- Define the recovery of your people, facilities and systems for every LOB
- Energize the SETA program
- Perform a gap assessment on all aspects of information security
- Draft ransomware vulnerability report

60 to 90 days

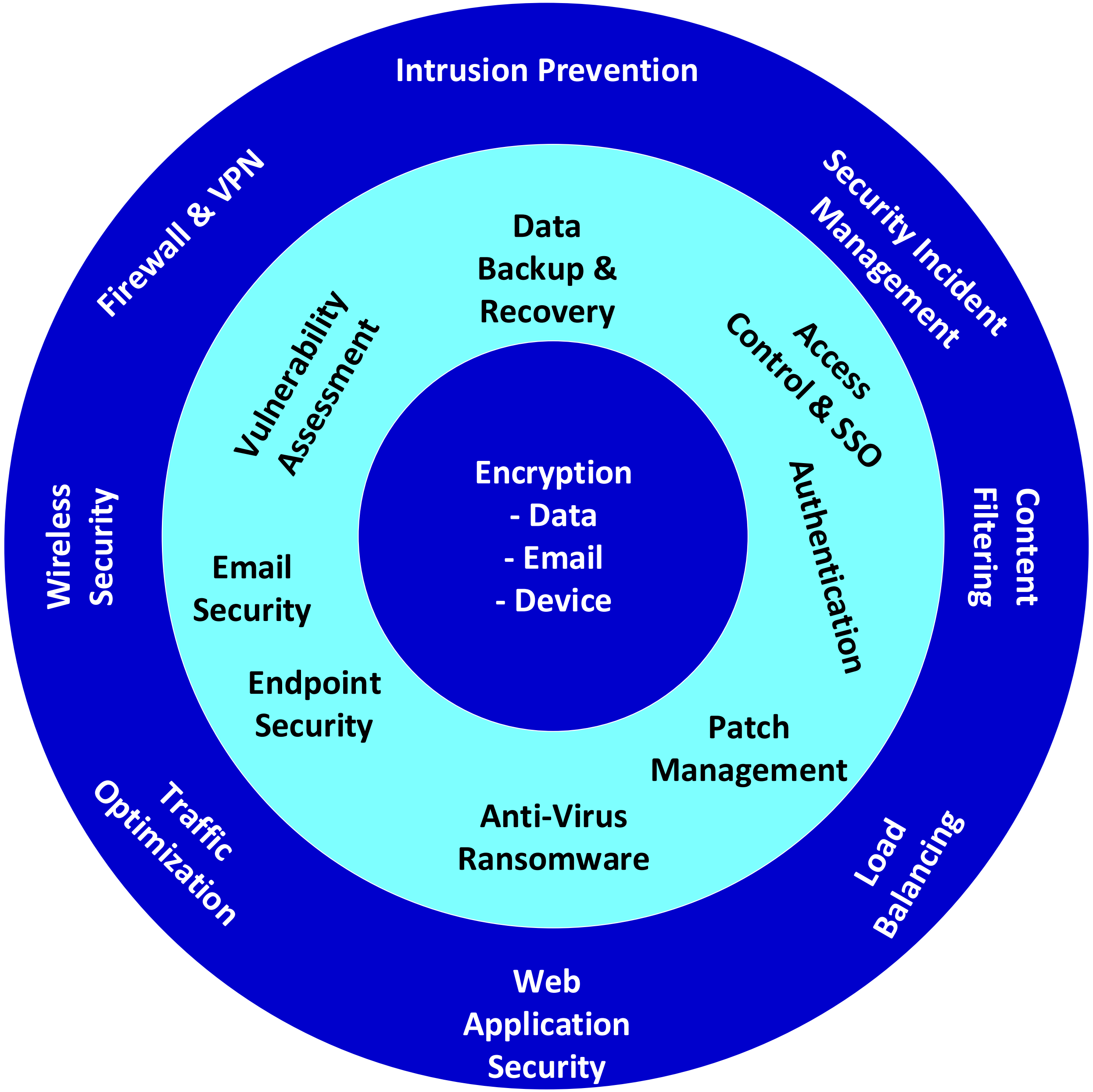
We all start at the same place, with the same plan.



Overlapping Layers

– A standard approach circa 2000 - 2017

– Today we want to see the AI inside!



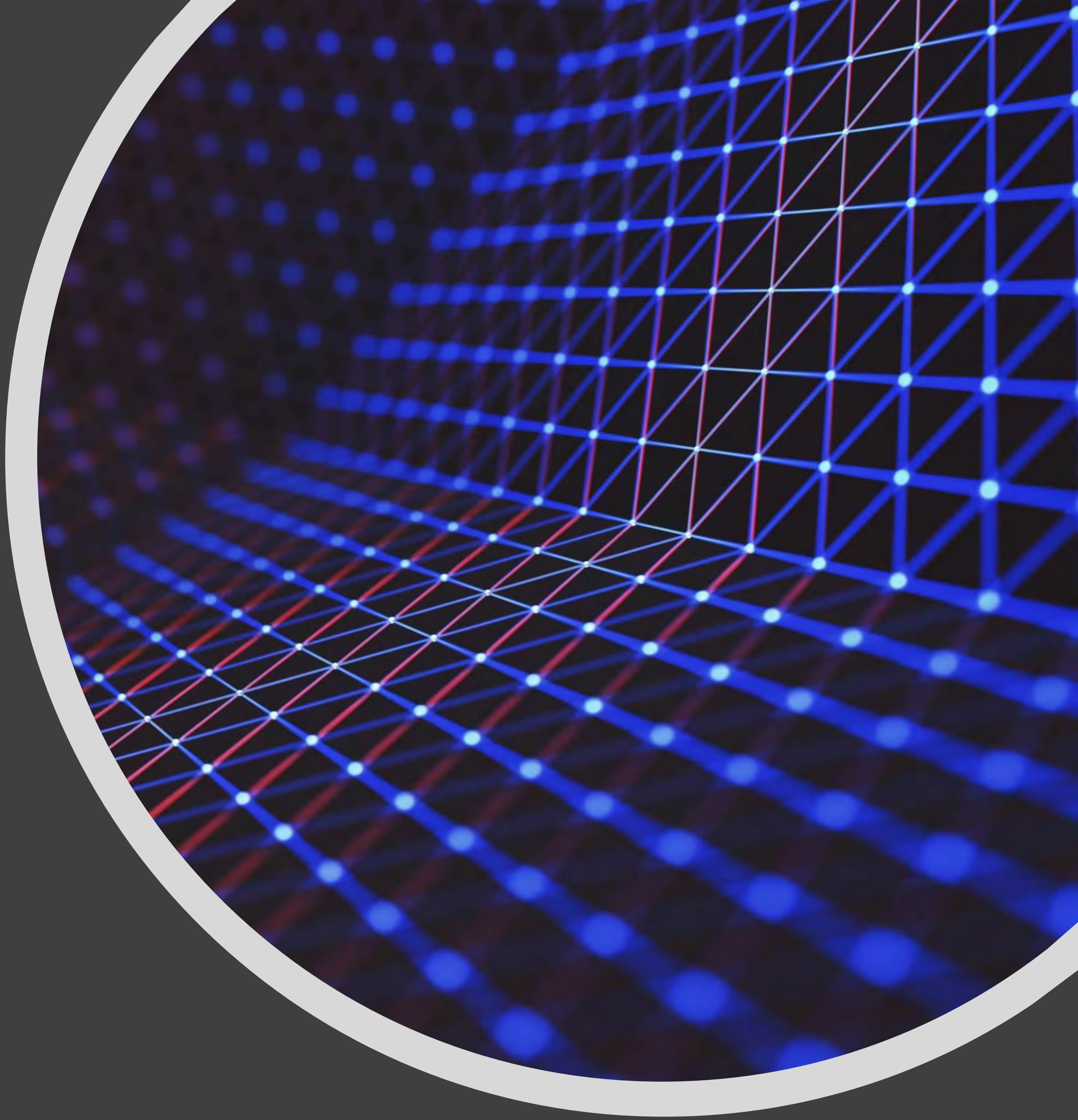
Cybersecurity is complex today

Agile

DevOps

Mobile

Websites are our busiest locations



CISO Skillset

1. Security Program Creation, Management, and Operations
2. Information Security Core Concepts (our domains)
3. Planning, Finance, Risk Management & Vendor Management
4. Governance, Risk & Compliance (GRC)
   Mind your 5 Ps
5. IT & IS Management Controls and Auditing
6. Technical Acumen

Assessing the Organization

- Organizational Maturity
- Operational Readiness

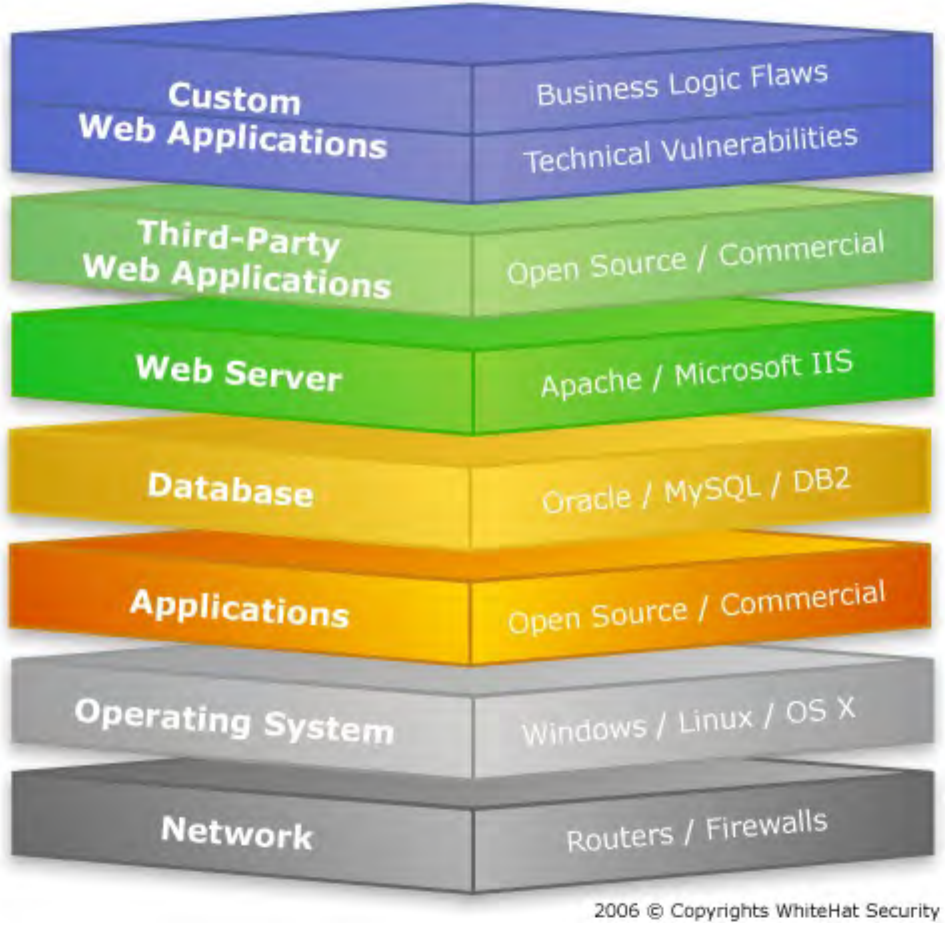
Level		Focus	Process Area	Result
5	Continually optimizing organizational competency	Continuous process improvement is fully operationalized at the enterprise level	- Organizational Innovation and deployment - Causal Analysis and Resolution - Change management competency is evident in all levels of the organization and is part of the organization's intellectual property and competitive edge.	Highest Level of: • cyber assurance • productivity • Quality • Responsiveness & • Profitability
4	Quantitatively managed organizational standards	Selection of a common approach & quantitative management in place	- Organizational process performance - Quantitative project management - Organization-wide standards and methods are broadly deployed for managing and leading change	Information Assurance
3	Defined processes & multiple project capability	Process standardization on best practices is evident	- Requirements Development - Technical solutions - Product integration - Verification - Validation - Organizational process focus & definition - Organizational Training - Integrated Project Management - Risk Management - Decision Analysis and Resolution - Comprehensive approach for managing change is being applied in multiple projects	
2	Managed but isolated projects	Basic project management using many different tactics used inconsistently	- Requirements management - Project planning, monitoring & control - Supplier agreement management - Quantitative measurement and analysis - Process & product quality assurance - Configuration and change management are applied in isolated projects	
1	Initial stage ad hoc or absent • planning • organization • control	Competent People and Heroics People dependent without any formal practices or plans	- Competent People and Heroics - Little or no change management applied	Highest rate of: • project failure • turnover • loss Lowest Level of: • productivity • quality

Scalability = Economic Flexibility

Scalability is the ability to adapt the size of the infrastructure to the ever-changing needs of the business.

Technology must be able to be expanded without the need for a forklift upgrade and should be able to scale back as needed.

Cybersecurity must maintain the CIA triad during the waxing or waning of the business.



2006 © Copyrights WhiteHat Security

One size does not fit all….

CREDIT: *DFWHC Foundation*

4 Points of Alignment

- Functionality
- Economic
- Talent
- Equipment | Existing or New
- Functionaity

Cybersecurity Road Map Artifacts

- Threat Hunting
- Log Aggregation
- Firewall Clustering
- Artificial Intelligence
- User Behavior Analytics
- Vulnerability Management
- Security Research
- Incident Response
- Forensics
- Training & Cross-training

Network & Endpoint Defenses

Are we monitoring multiple layers of security?

- Firewalls
- Data Loss Protection
- Spam Filtering
- Antivirus
- Threat Emulation
- HTTPS Inspection
- Bot Protection
- Application Control
- URL Filtering

Is it enough?

- Nothing is Foolproof
- There is no magic bullet
- With time and money, anything can be breached
- Users make mistakes
- Vendors make mistakes

What we don´t see can kill us

- Brute force attacks on all assets
- Brute force on local accounts
- Detection evasion – local event log deletion
- Privilege escalation
- Lateral movement
- New local user accounts created
- Protocol poisoning

How do we gain insight?

- Artificial Intelligence?
- Machine Learning?
- Cluster Algorithms?
- Additional Staff?
- Specialized Applications?

AI and Behavioral Analytics

- Learns what your network traffic looks like
- Connects the dots from all the, many, many logs
- Detects the anomalies that look like legitimate traffic
- Exposes intruders
- We see all the water molecules in the flowing river

Use the AI Inside

- Scans our network for all devices
- Detects new devices
- Performs vulnerability assessments on those devices
- Advises us of those vulnerabilities, and the context in which they are a threat to our organization
- Creates remediation workflows and tracking

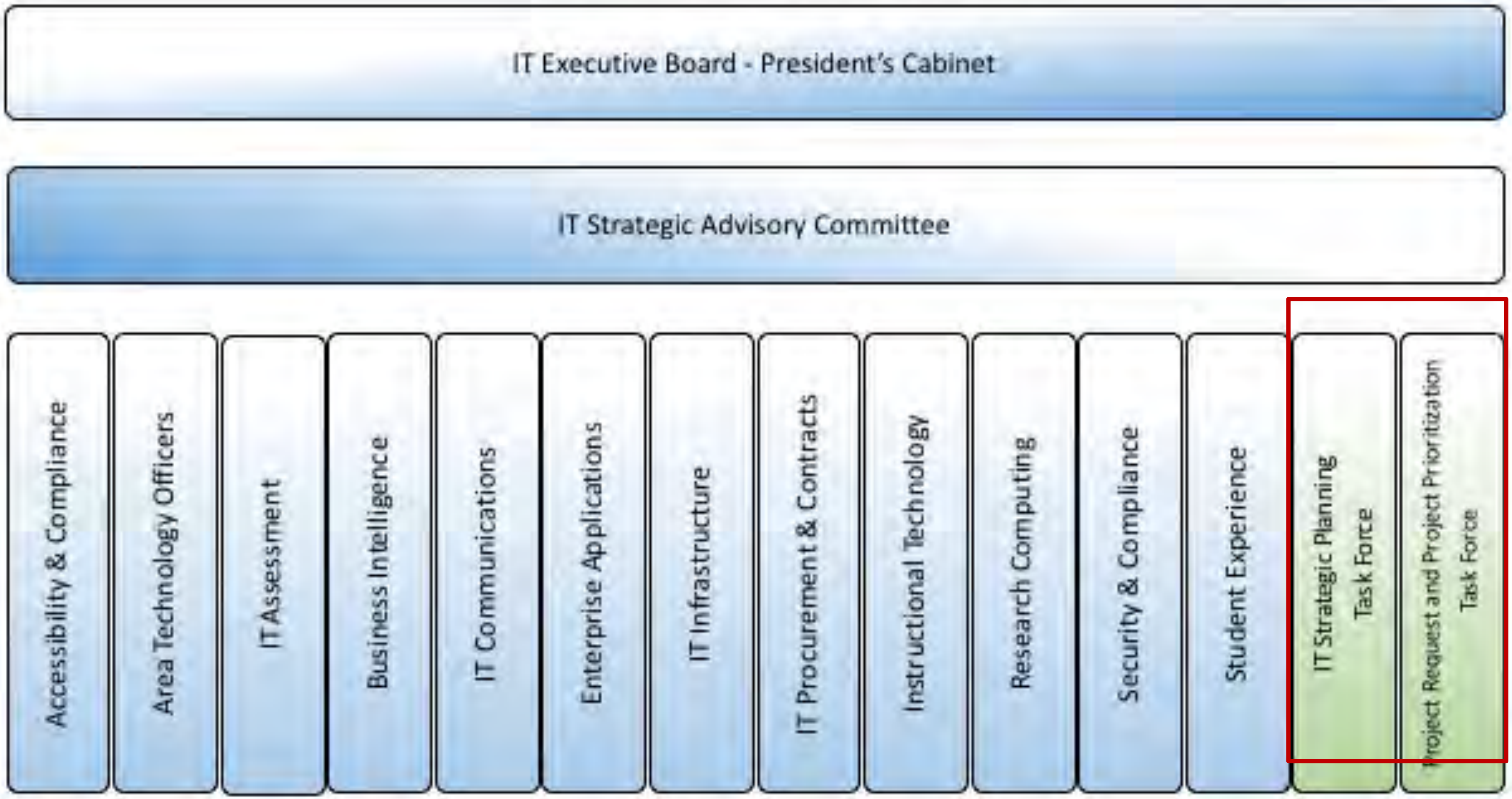
Benefits?

- Keeps vulnerable systems on our radar
- Vulnerability notifications
- Remediation tasks are assigned to system owners
- Track remediation progress
- Makes vulnerability management workable
- Decreases attack surface

A CISO's success hinges on the success of the cybersecurity *team* monitoring the central nervous system of the organization and reporting its findings to senior management and the board.

Communication vs. Speculation

IT Governance



IT Executive Board - President's Cabinet

IT Strategic Advisory Committee

- Accessibility & Compliance
- Area Technology Officers
- IT Assessment
- Business Intelligence
- IT Communications
- Enterprise Applications
- IT Infrastructure
- IT Procurement & Contracts
- Instructional Technology
- Research Computing
- Security & Compliance
- Student Experience
- IT Strategic Planning Task Force
- Project Request and Project Prioritization Task Force

Board Reporting

The Board of Directors (the “Board”)is 100% responsible for the organization and every action or inaction of the organization.

Regulatory guidance in many industries suggests that the Board must be actively engaged in the oversight of the information security program.

It is critical to the success of any cybersecurity program that the board to set the
“***tone-from-the-top***”.

Regulatory guidance stresses the need for both senior management and the board to be actively involved.

Board Reporting

Clear and descriptive reporting is extremely important

Every organization must document their reporting expectations

- Frequency of reporting,
- GRC (governance risk compliance) meetings
- Any expectations for stakeholder participation

BEST PRACRTICE

The best methodologies for creating a framework for active involvement by the board, senior management and key stakeholders is to create a reporting framework that engages all parties.

Board Reporting

Cybersecurity Board reports should include:

- Total inventory of actively managed assets
- Status of threat | vulnerability | patch management triad
- Status of the organization's cybersecurity risk assessments
- Ongoing monitoring activities
- Any material upcoming, contract renewals, terminations or notable problems with vendors.

Board Reporting

I always recommend board reports contain two fundamental components.

A PowerPoint slide deck one slide devoted to each pillar of information security risk management

1. Asset Security
2. Security Architecture and Engineering
3. Communication and Network Security
4. Identity and Access Management (IAM)
5. Security Assessment and Testing
6. Security Operations
7. Software Development Security
8. Business Continuity Management

Board Reporting

The other component I recommend is a document containing a narrative on each of the cybersecurity pillars as well as

- Important industry information
- New regulatory guidance
- Updates on investments in staff, staff training, key additions or departures from the team
- An overall inventory of actively managed third party network connections, any upcoming connections
- Any material cybersecurity program changes particularly focusing on any changes in high risk or critical areas of operation.

Frameworks are your friends

- Use a framework!
- There are many to choose from.
- COSO Framework
- NIST
- ISO

ASSESS

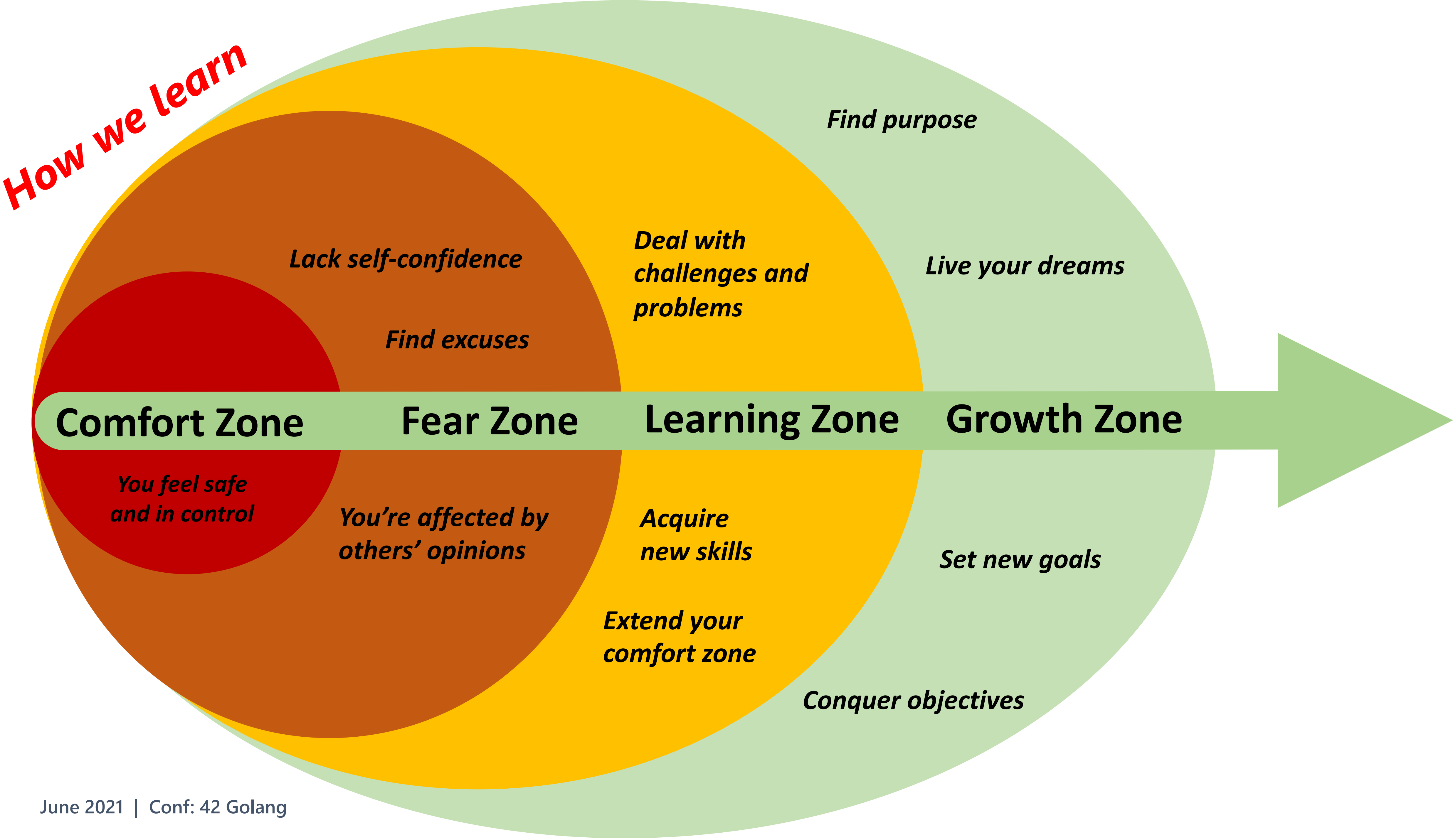
1. Risks (Inherent & Residual)
2. People | Processes | Technology
3. Talent level
4. Project management capability
5. Standardization
6. Quantitative management capability (Golden Circle)

Person	Role	Skill	Current Capability (5 scale)	Ideal Capability	Developmental Action
Jane	Current Role	Skill 1	3	3	None
Alice	Current Role	Skill 2	2	3	Training
Kim	Current Role	Skill 3	1	3	Training
Johnny	Current Role	Skill 4	4	3	Mentor
Carl	Current Role	Skill 5	5	4	Mentor
Ralph	Current Role	Skill 6	2	4	Training
Sara	Current Role	Skill 7	3	4	Training
None		Skill 8	0	5	Partner
None		Skill 9	0	5	Hire

Certifications

$(ISC)^2$	Cisco	SANS
- CISSP - SSCP - CCSP - CAP - CSSLP - HCISPP - CISSP - ISSAP/ISSEP/ISSMP	- CCENT - CCT - CCDA - CCNA - CCNP - CCDE - CCIE	Et al…

How we learn



Comfort Zone

You feel safe and in control

Fear Zone

Lack self-confidence

Find excuses

You're affected by others' opinions

Learning Zone

Deal with challenges and problems

Acquire new skills

Extend your comfort zone

Growth Zone

Find purpose

Live your dreams

Set new goals

Conquer objectives

Frameworks

Framework	Best Utilization
NIST CSF	Cybersecurity
CMM	Software Development
COSO	Enterprise Risk Management
COBIT	IT Governance/Controls
ITIL/ITSM	IT Service Management
ISO/IEC 27001	Cybersecurity
TOGAF	Enterprise Architecture
Zachman	Enterprise IT

The clock in your head

What	Time
1. Justify your technology	1. 18 months
2. Train, train, train	2. 3 months
3. Calendar up	3. Monday mornings
4. GRC	4. Monthly
5. Framework adjustments	5. 12-18 months NMW or PRN
6. GA release	6. 12-18 months NMW or PRN
7. Vulnerability Assessments	7. Daily

Keeps on ticking…

What	Time
8. Risk Assessments	8. Annually and PRN
9. Code reviews	9. DevOps is a team sport
10. Patches	10. Weekly and PRN
11. System Configuration	11. PRE-production

Cybersecurity Road Map for any size corporation

1. SETA
2. Who are your stakeholders
3. Watch your numbers
   a. Budget, Number of Employees, Burn Rate
4. Know your 4 P’s
   (policy, procedure, process, project)
5. Security architecture
6. Asset ID
7. BCP/DRP
8. Risk Management
9. Training & Cross-training

5 Areas where successful CISOs accel!

1. IQ and EIQ
2. Communication
3. Technical Kung Fu vs. Krav Maga
4. High performance team building
5. Third Party Risk Management

Prep

- 30-60-90 day plan
- Manager’s expectations
- Org chart
- Industry R&D
- Company R&D
- Department R&D

- 10 days

Measure

- Strategic & tactical plans (Policies & Procedures)
- Budget
- GRC (P&P Analysis)
- Enterprise Information Architecture
- Assets being managed
- Assets unmanaged
- Vulnerability Assessment Processes
- Personnel skill set
- Access Controls
- Interview key stakeholders
- Interview Internal Audit, external audit & Compliance

0 to 30 days

Assess

- Enterprise cybersecurity architecture vs. baseline
- Current training plan(s)
- Software development team(s)
- DevOps Team(s)
- How the organization is meeting PCI, HIPAA, CCPA, NTDFS
- Network security audit results
- Any outstanding findings from prior cybersecurity audits/exams
- Physical security
- Assess the Business Continuity Management Plan
- Assess corporate backup management strategy

30 to 60 days

Plan

- Create Corporate Information Protection Plan
- Create Information Security Strategic Plan for the coming year
- Build you
- Social your roadmap
- Plan test of RTO, RPO, and MAD
- Define the recovery of your people, facilities and systems for every LOB
- Energize the SETA program
- Perform a gap assessment on all aspects of information security
- Draft ransomware vulnerability report

60 to 90 days

MAP

Measure • Assess • Plan

- Assess the information security department, the people in it and the organization it serves.
- Develop organization specific tools to accurately determine the capabilities and operational readiness of the department.
- Create the people, processes and technology road map for the information security department

MAP

Measure • Assess • Plan

MEASURE

- Cybersecurity department
- The people
- The organization it serves.

MAP

Measure • Assess • Plan

The First 100 Days

ASSESS

- Cybersecurity department
- The people
- The organization it serves.

MAP

Measure • Assess • Plan

The First 100 Days

Plan

- Cybersecurity department
- The people
- The organization it serves.

Assessment

- Organization
- Cybersecurity Team
- Information Technology Team
- Third Parties [Vendors]

Plan the work.

Work the plan.

- Strategic
- Tactical

Plan the work.

Work the plan.

Measure progress

Demonstrate

Program effectiveness

Process effectiveness

Level of security

MAP

Measure • Assess • Plan

- Industry
- Organization’s life cycle position
- Industry expanding or contracting
- Disruption potential
- Critical infrastructure designation
- Your level of culture shock…

Operational Readiness

Business Continuity & Disaster Recovery

- BIA
- RPO
- RTO
- MAD

Business Impact Analysis

- Everyone can’t be #1
- Define criticality 1st
- The “tone-from-the-top”

Business Continuity Management

Business Continuity

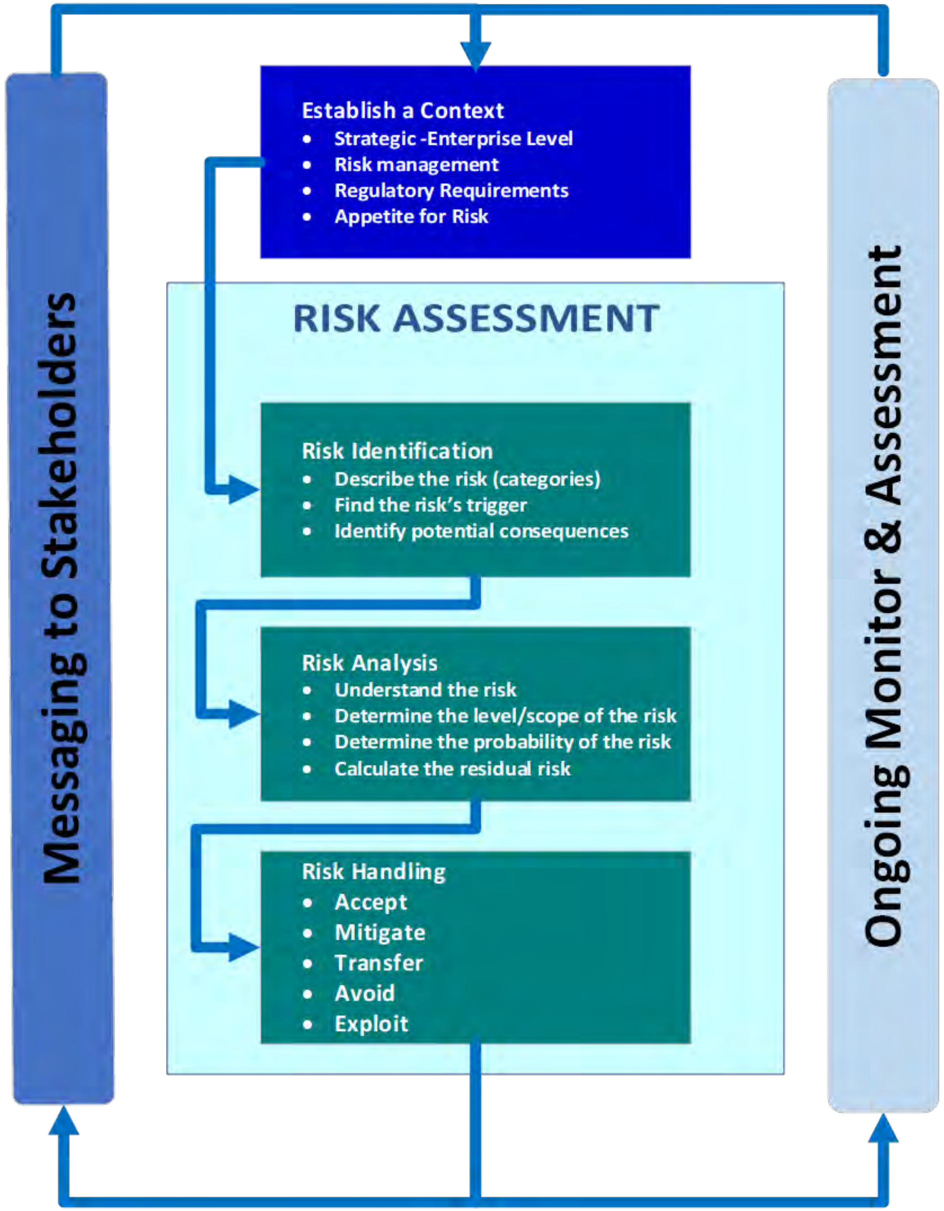
- Disaster Recovery
- Pandemic Planning
- Incident Response

Disaster Recovery’s Three Steps

Recover

1. People
2. Facilities
3. Systems

Cybersecurity Risk Assessment Process



Messaging to Stakeholders

Establish a Context
- Strategic -Enterprise Level
- Risk management
- Regulatory Requirements
- Appetite for Risk

RISK ASSESSMENT

Risk Identification
- Describe the risk (categories)
- Find the risk's trigger
- Identify potential consequences

Risk Analysis
- Understand the risk
- Determine the level/scope of the risk
- Determine the probability of the risk
- Calculate the residual risk

Risk Handling
- Accept
- Mitigate
- Transfer
- Avoid
- Exploit

Ongoing Monitor & Assessment

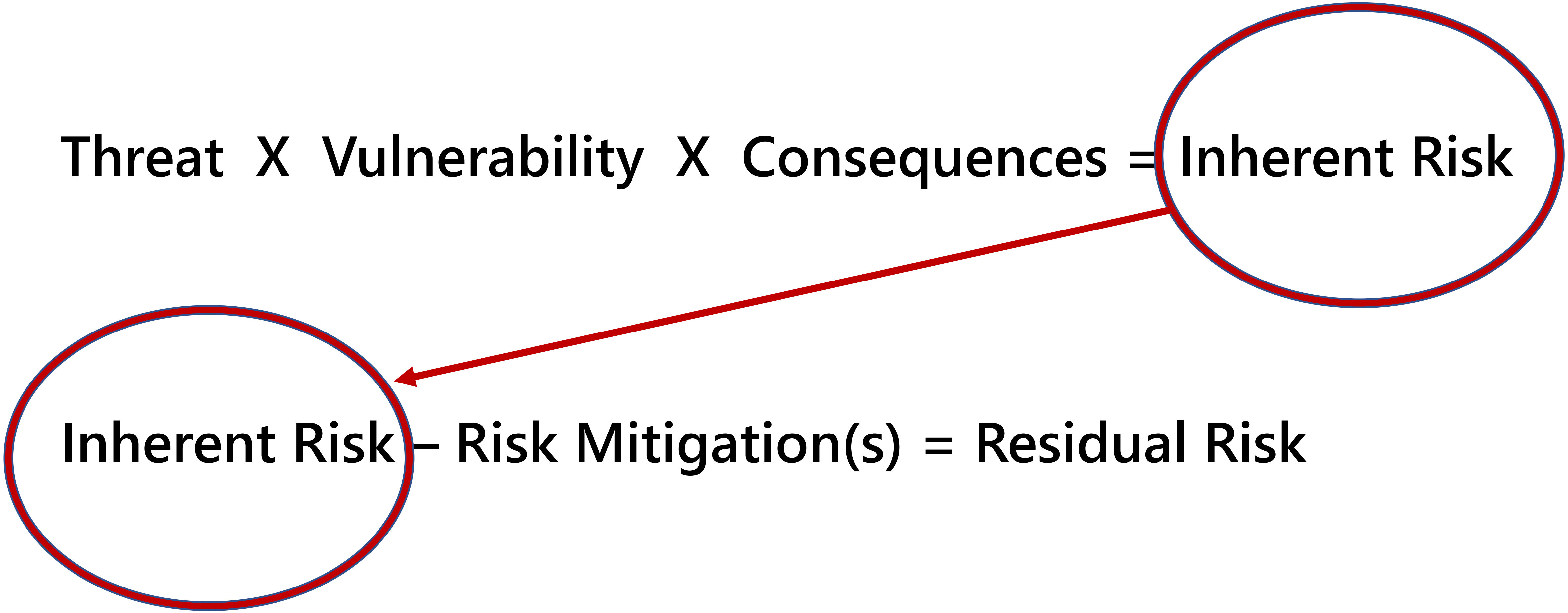
Risk Analysis

Risk Appetite | Risk Appetite Statement

Threat X Vulnerability X Consequences = Inherent Risk

Inherent Risk – Risk Mitigation(s) = Residual Risk

Risk Analysis



Threat X Vulnerability X Consequences = Inherent Risk

Inherent Risk – Risk Mitigation(s) = Residual Risk

Simple Risk Modeling

Inherent Risk	**-**	**Impact of Risk Controls**	**=**	**Residual Risk**
A Risk **(Any Risk)**	**-**	**Risk Controls**	**=**	**Residual Risk**

Example #1

Environmental Risk

1	Natural Disaster Earthquake in Oklahoma (circa 2014)	**-**	Disaster Recovery Site more than 100 miles away	**=**	Probability of downtime before recovery site comes online
	100%	**-**	**80%**	**=**	**20%**

Example #2

2	Natural Disaster Earthquake in Oklahoma (circa 2019)	**-**	Disaster Recovery Site more than 100 miles away	**=**	Probability of downtime before recovery site comes online
	10%	**-**	**9%**	**=**	**1%**

	A Risk (Any Risk)	The Harm or Loss of Any Single Risk (1 to 10)	X	Probability of the Risk's Occurrence (1 to 10)	=	Inherent Risk Score	-	Applied Risk Controls (Risk Mitigation)	Risk Controls Value	=	Residual Risk		Final Risk Rating
Environmental Risks Assessed													
1	**Natural Disaster Earthquake in Oklahoma**	5	X	8	=	40	-	Disaster Recovery Site more than 100 miles away	20	=	20		Low Risk
2	**Man-made Disaster (Arson)**	9	X	9	=	81	-	Advanced dry pipe sprinkler system installed and operational.	45	=	36		Below Average Risk
Regulatory Guidelines for Risk Categories													
3	**Strategic Risk** (of any vendor)	9	X	9	=	81	-	Nothing can be done to reduce this risk	0	=	81		High Risk
4	**Reputational Risk** (of any vendor)	8	X	10	=	80	-	Hire a social media consultant	5	=	75		Above Average Risk
5	**Financial Risk** (of any vendor)	8	X	8	=	64	-	Ongoing monitoring of Edgar and D&B	5	=	59		Average Risk
6	**Operational Risk** (of any vendor)	10	X	10	=	100	-	Backup item processing system in place	35	=	65		Above Average Risk
7	**Compliance Risk** (of any vendor)	5	X	10	=	50	-	Complaisance department will audit all Bus	15	=	35		Below Average Risk
⋮											0		
nth	**Category**	10	X	10	=	100	-	Control that works	80	=	20		Low Risk

Vendor Risk Assessment

All Vendors

As of: January 1, 2019

Risk Score	Risk Categories
0 – 20	Low Risk
21 - 40	Below Average Risk
41 - 60	Average Risk
61 - 80	Above Average Risk
81 - 100	High Risk

Vendor Name	Potential Risk to Your Organization	Risk of Harm or Loss 1 to 10 Low to High	Probability of Risk's Occurrence 1 to 10 Low to High	Inherent Risk Score	Raw Risk Rating	Risk Control Action(s)	Mitigation Value	Mitigated Risk Score	Mitigated Risk Category
AT&T	Internet Service Provider	9	10	90	High Risk	Two ISPs ATT&T and Cox	50	40	Below Average Risk
ATM & FI Equipment Service Provider	Installation & repair of ATMs & FI's equipment	7	8	56	Average Risk	ANY has two vendors that produce cards	10	46	Average Risk
Braintree	Mobile and web payment systems	10	7	70	Above Average Risk	Backup system in place	50	20	Low Risk
Ceridian	Dayforce - employee self-service functions	8	6	48	Average Risk	Ceridian utilizes Tier 4 datacenters	25	23	Below Average Risk
Dell	Computer hardware	5	5	25	Below Average Risk	This application resides on ANY's network and source code is escrowed	1	24	Below Average Risk
Harland/Clarke	Check programs	2	2	4	Low Risk	Alternate check provider available with one call	1	3	Low Risk
Jack Henry & Associates	Xperience core banking system software	10	4	40	Below Average Risk	JHA utilizes multiple datacenters	20	20	Low Risk
Janitorial/Cleaning	Exposure to nonpublic personal information inside the FI	3	3	9	Low Risk	Alternate cleaning crew available	1	8	Low Risk
Microsoft	Computer software	10	2	20	Low Risk	No immediate substitute available	0	20	Low Risk
Q2	Digital & mobile banking	6	9	54	Average Risk	Alternate service provider available	10	44	Average Risk
Salesforce	CRM platform (cloud based)	5	5	25	Below Average Risk	Ongoing monitoring program in place	10	15	Low Risk
SAS Institute	Customer analytics	8	8	64	Above Average Risk	Ongoing auditing of vendor in place	10	54	Average Risk
Stripe	Credit card issuing technology, point-of-sale software and a billing platform	8	8	64	Above Average Risk	Alternate vendor in place	25	39	Below Average Risk
Upstream Correspondent Bank	Treasury services and foreign exchange	5	5	25	Below Average Risk	Alternate correspondent bank agreement in place	15	10	Low Risk
YapStone	End-to-end payment solutions	9	8	72	Above Average Risk	Alternate solution provider agreement in place	25	47	Average Risk
Averages		**7**	**6**	**44**	Average Risk	**Averages**	**17**	**28**	Below Average Risk

Change Management

- SDLC
- Data warehouse and data marts
- Information factory
- Agile
- Digital transformation
- DevOps
- AI
- IoT

How do we adapt since we really have no logical alternative?

- Skills – Hard & Soft
- Your comfort zone
  (technology and people)
- Surround yourself with smarter people

Measure

What	With
Skills	Skill matrix
EIQ	Any
Risk appetite	COSO framework
Obsolescence	Asset management

Assess Team Composition

-**Hard skills** [skill matrix]

-**Soft skills** [Myers–Briggs or True Colors]

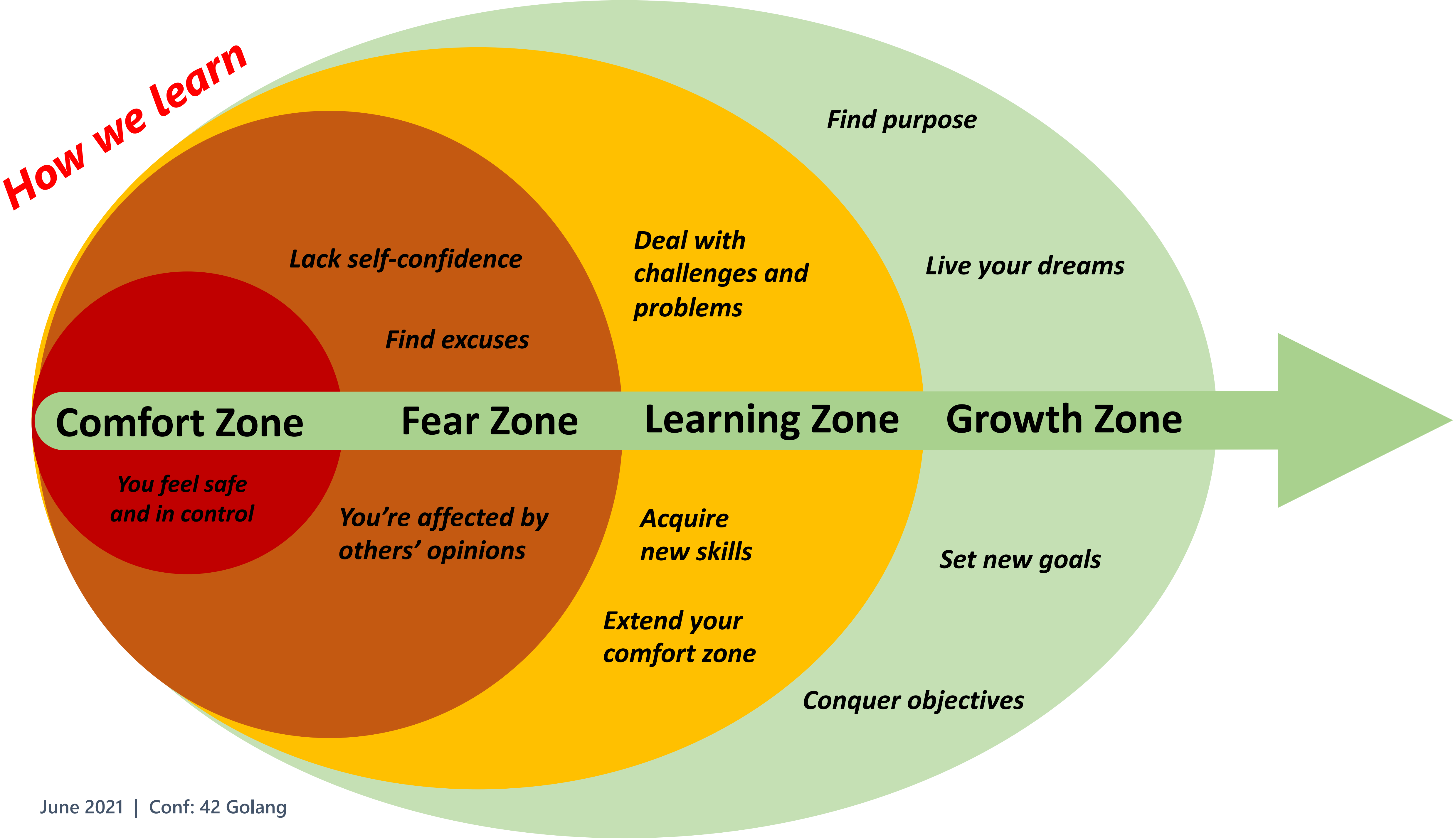
Be willing to invest in the team

- Training & Education
- Get them certifications
- Get more than one!
- (ISC)^2 has a few…

Certifications

(ISC)^2	Cisco	SANS
- CISSP	- CCENT	Et al…
- SSCP	- CCT	
- CCSP	- CCDA	
- CAP	- CCNA	
- CSSLP	- CCNP	
- HCISPP	- CCDE	
- CISSP - ISSAP/ISSEP/ISSMP	- CCIE	

How we learn


Find purpose
Lack self-confidence
Deal with challenges and problems
Live your dreams
Find excuses
Comfort Zone
Fear Zone
Learning Zone
Growth Zone
You feel safe and in control
You're affected by others' opinions
Acquire new skills
Set new goals
Extend your comfort zone
Conquer objectives

Final Thoughts

1.	Wire	1.	Get it right up front
2.	Memory	2.	You can’t have too much
3.	SSD	3.	Spinning disks? Why?
4.	Asset Management	4.	You MUST know what’s attached to your network and what you’re tasked with protecting!
5.	Personnel	5.	People are your best assets. Care for them like they are family.

CISA Releases Best Practices for Preventing Business Disruption from Ransomware Attacks

Filtering network traffic to prohibit ingress and egress communications with known malicious IP addresses;

Enabling strong spam filters to prevent phishing emails from reaching end users;

Implementing robust network segmentation between information technology and operational technology networks; and

Regularly testing manual controls; and ensuring that backups are implemented, regularly tested, and isolated from network connections.

Stone Creek
COACHING

Gordon Rudd
Chief Vision Officer
Stone Creek Coaching
+1 (918) 640-5706
Gordon@stonecreekcoaching.com

Tech Career Designer & Executive Coach to
CISOs | CIOs | CTOs | Author | Keynote Speaker

Stone Creek Coaching provides career designs for CISOs, CIOs & CTOs and technical career coaching through individual one-on-one sessions | Masterminds | Hugh Performance Team Building