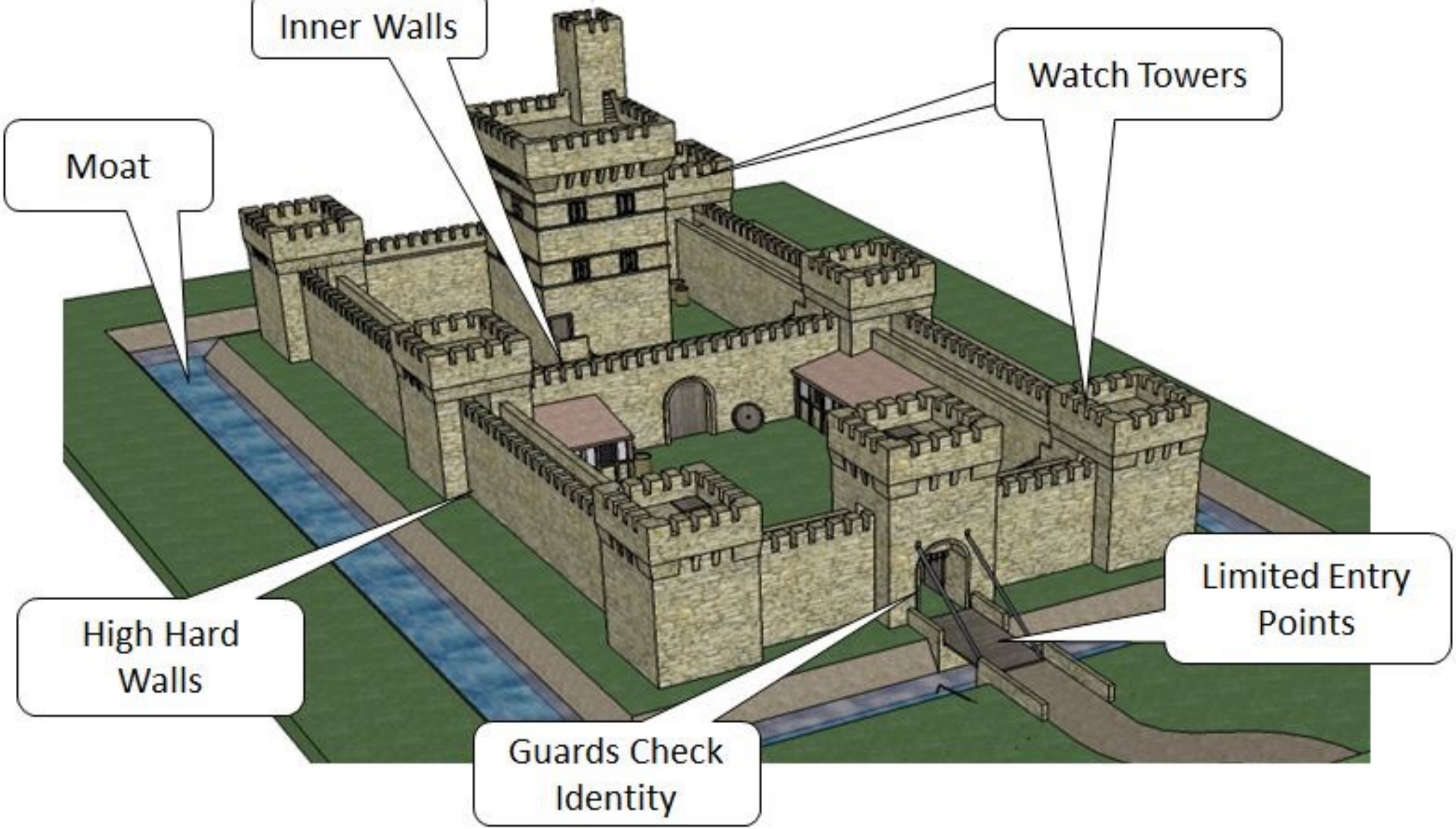
Conf 42: Python 2021

Creating scalable, sustainable cybersecurity for any size organization

AGENDA

1. **Define the relationship between scalability, sustainability and flexibility required in any cybersecurity program/department.**
2. **Assessing your program’s cybersecurity’s operational readiness.**
3. **Successfully communicating with your GRC teams, C-Suite, and Board.**
4. **Identify and focus on the top five areas CISOs need to be successful.**

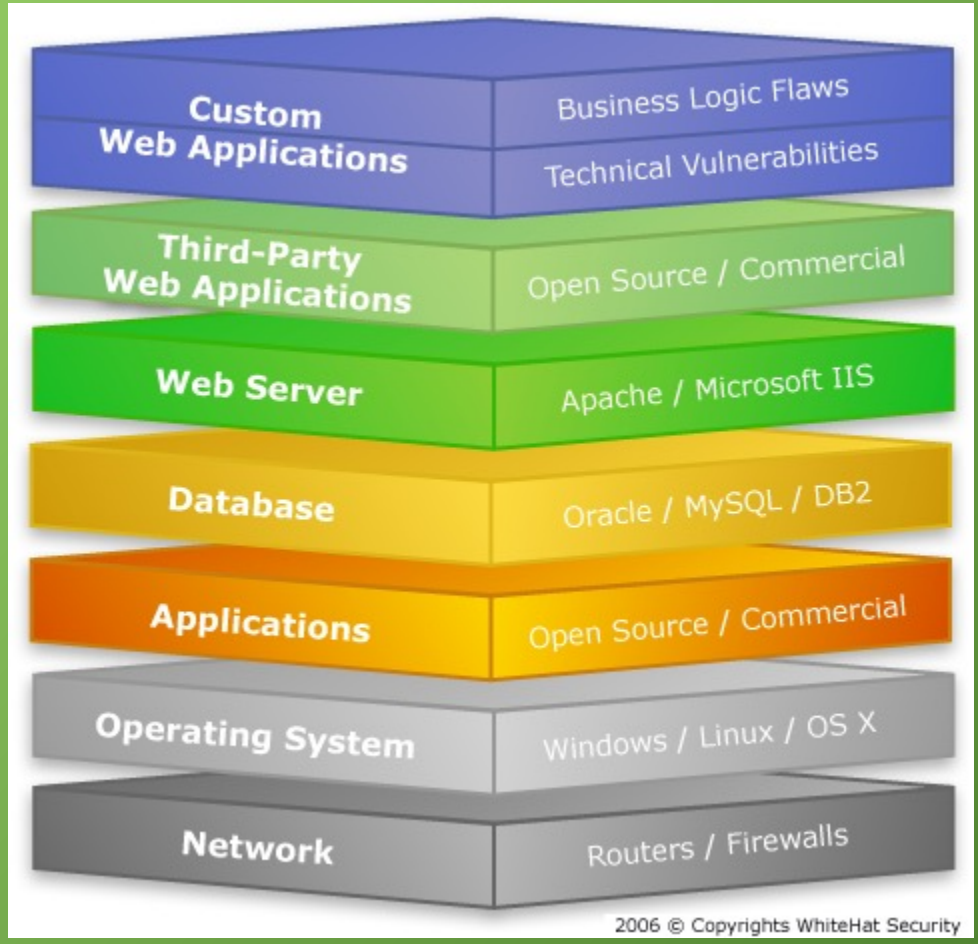

Inner Walls
Watch Towers
Moat
High Hard Walls
Limited Entry Points
Guards Check Identity

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.



What’s your cybersecurity readiness?

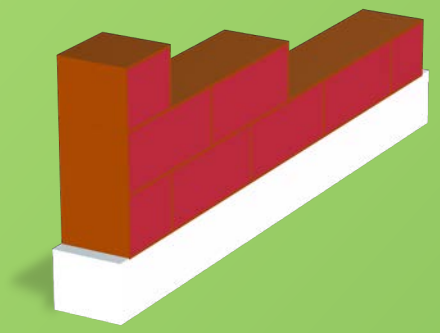
SOC or No SOC?

SETA

Security Education Training & Awareness

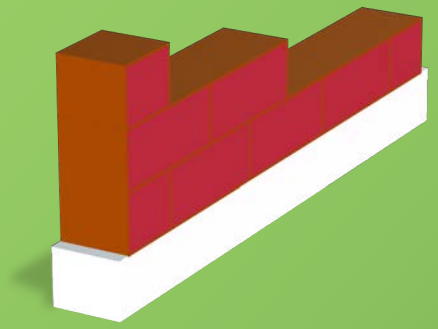
Milestone 1

Identify your stakeholders



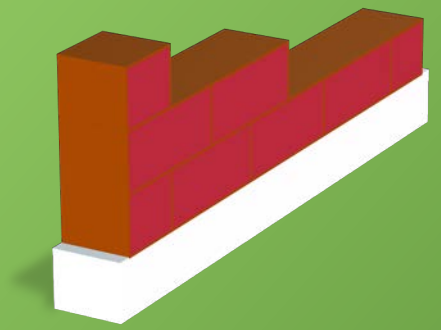
Milestone 2

Understand your numbers



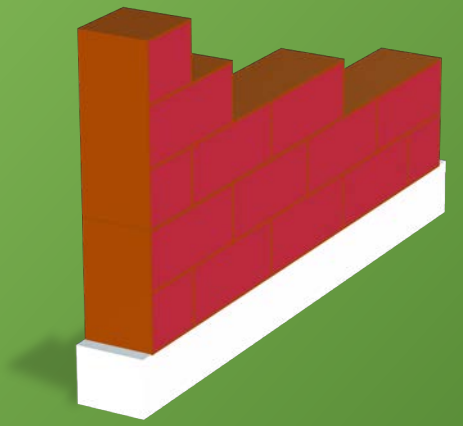
Milestone 3

GRC’s 5 P’s



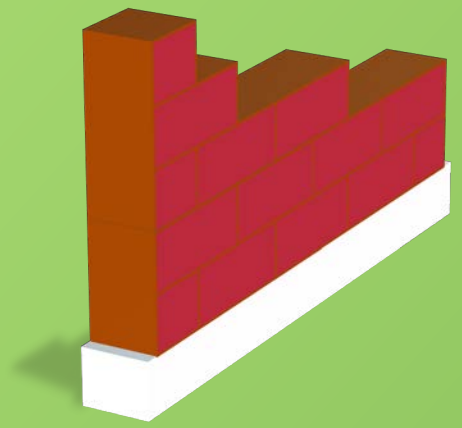
Milestone 4

Security Architecture



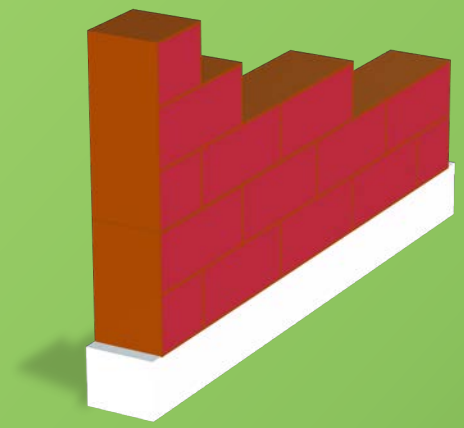
Milestone 5

Asset ID



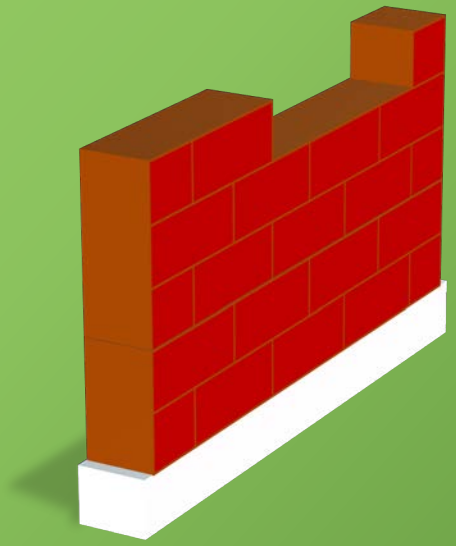
Milestone 6

BCP / DRP



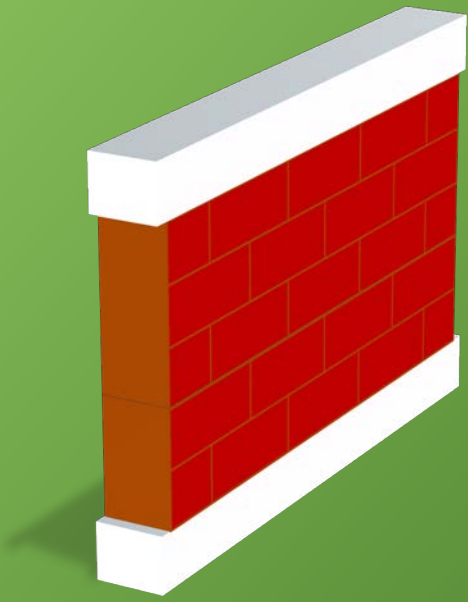
Milestone 7

Risk Management



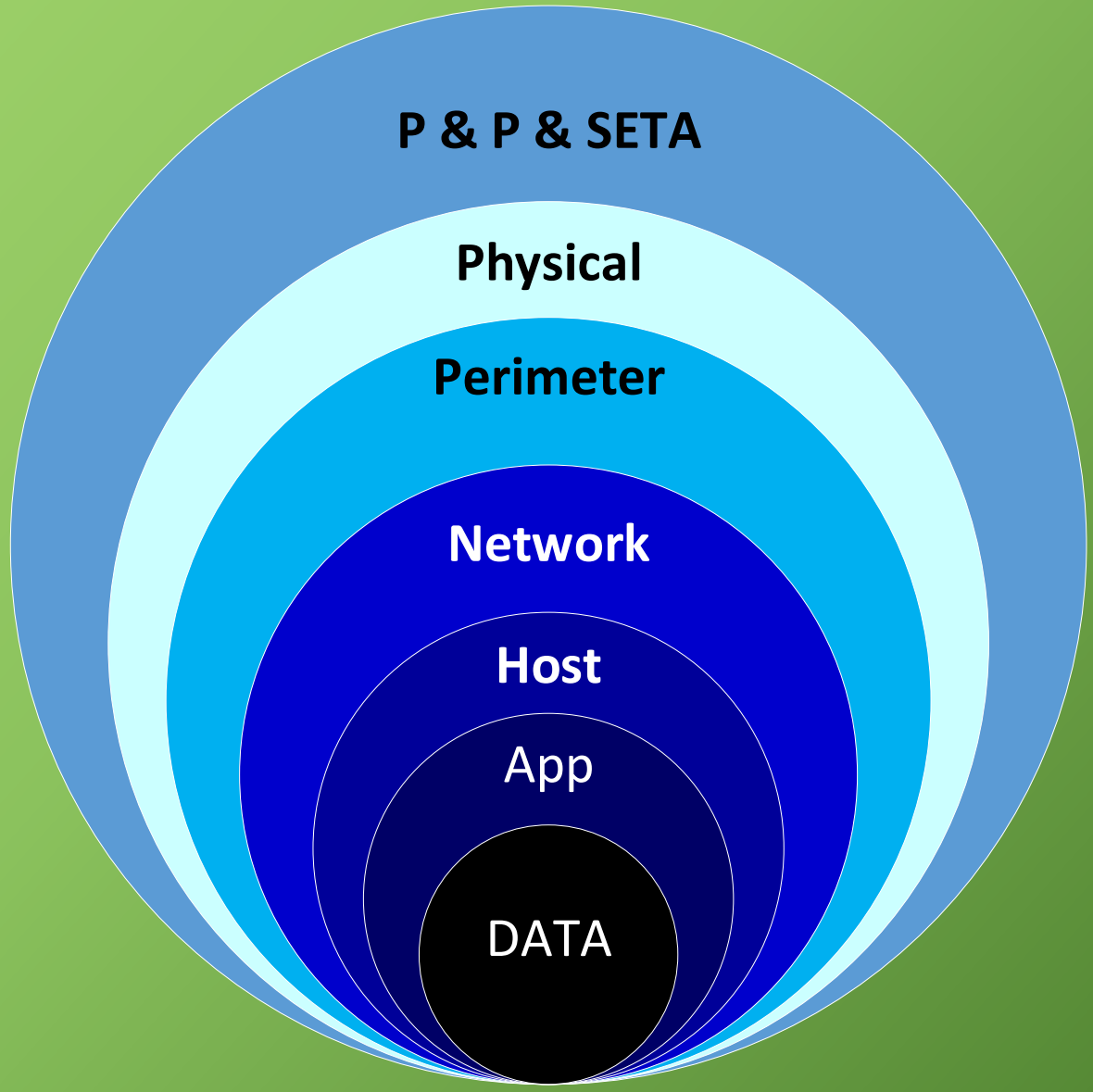
Milestone 8

Training & Cross Training



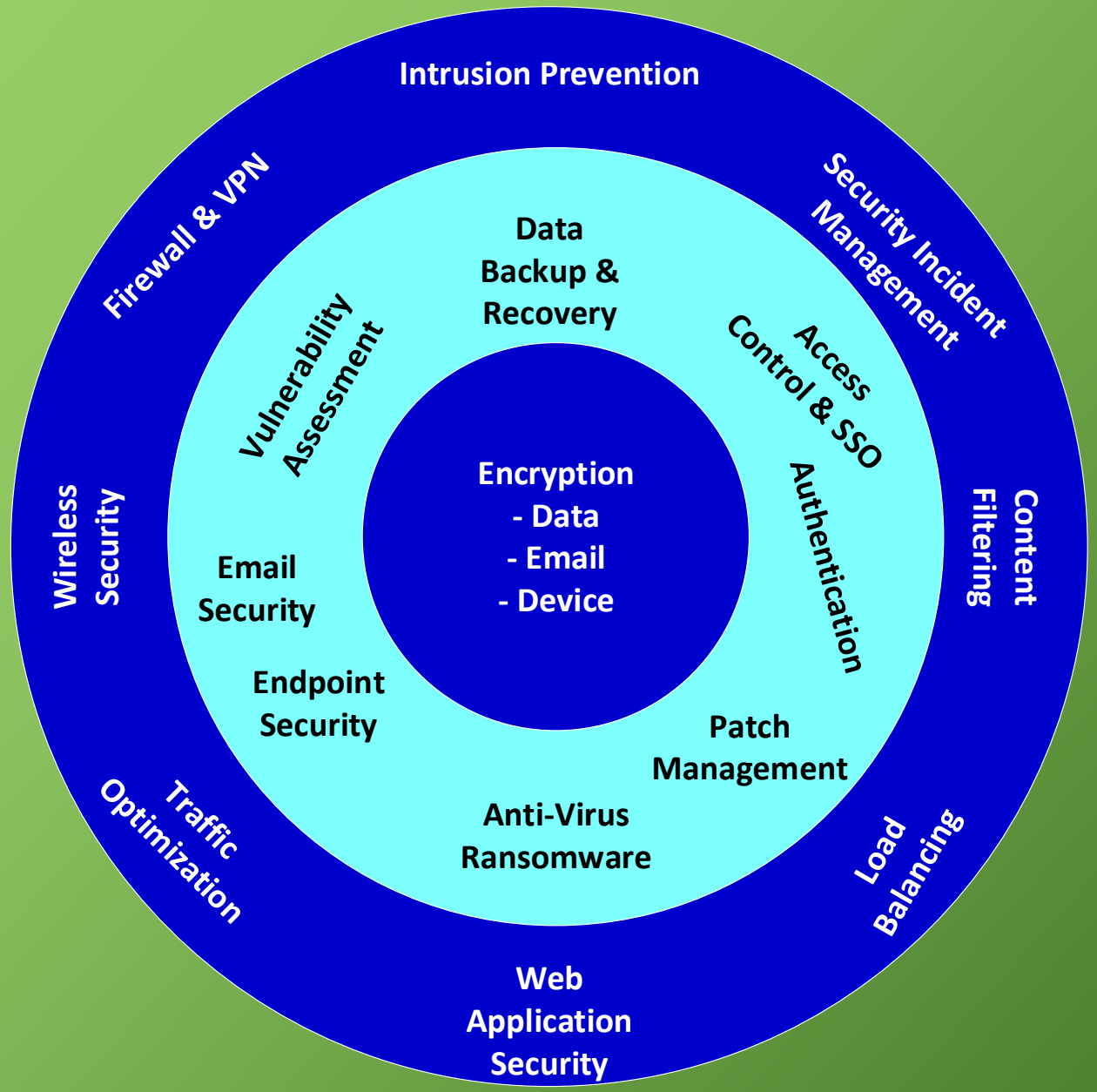
Milestone 9

We all start at the same place, with the same plan…right?



Overlapping Layers

- A standard approach circa 2002-2017
- Today, we want to see the AI inside!



Layered Security Model - 1st Layer

Security Incident Management

Web App Security

Content Filtering

Load Balancing

Traffic Optimization

Intrusion Prevention/Detection

Firewall & VPN

Wireless Security

Layered Security Model - 2nd Layer

Threat Intelligence	Access Control	Email Security
Vulnerability Assessment	Authentication	Backup & Recovery
Patch Management	End Point Security	

Layered Security Model - 3rd Layer

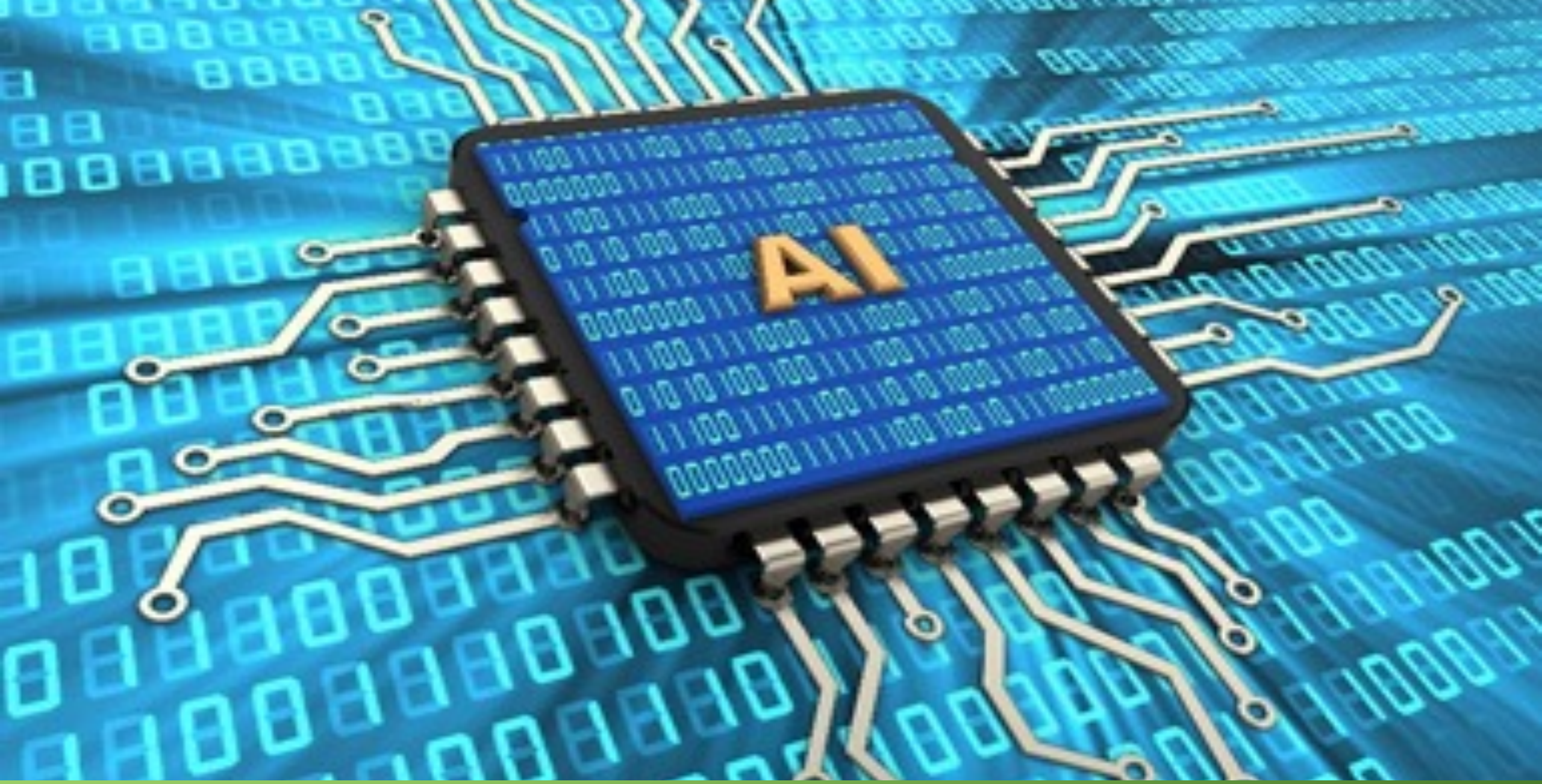
Data Encryption

Email Encryption

Device Encryption

Layered Security Model

Incident Management	Web Application Security	Content Filtering	Load Balancing	Traffic Optimization	Intrusion Prevention/ Detection
Firewall VPN	Vulnerability Assessment	End Point Security	Data Backup & Recovery	Authentication	Access Control
Wireless Security	Patch Management	Email Security	Data Encryption	Email Encryption	Device Encryption


AI

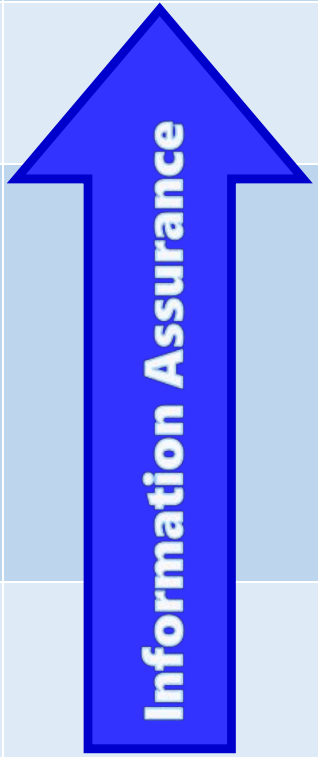
One size does not fit all….

CREDIT: *DFWHC Foundation*

Communicate or Speculate

The choice is yours

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	
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

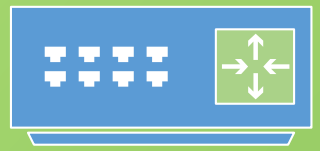


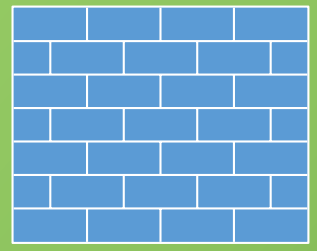
- Information Security
- Cyber Security
- Information Assurance
- Cyber Assurance
- GRC

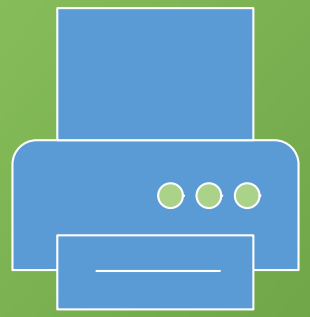
Small Businesses

How do you focus on cybersecurity with all the other “more pressing issues” you have to deal with everyday as a small business owner?

Level 1







- Economic
- Talent
- Existing Equipment
-  Function

4 Points of Alignment

Routers? What's a router?

- Is it an 802.11b, 802.11g, 802.11n, or 802.11AC?
- Single band vs Dual band vs Tri-Band (2.4GHz, 5GHz and 5GHz)
- Speed
  - 802.11b - up to 11Mbps
  - 802.11g – maximum 54Mbps
  - 802.11n - maximum 300Mbps [probable max = 100Mbps
  - 802.11AC – maximum 5300Mbps

Routers, you're not confused...yet?

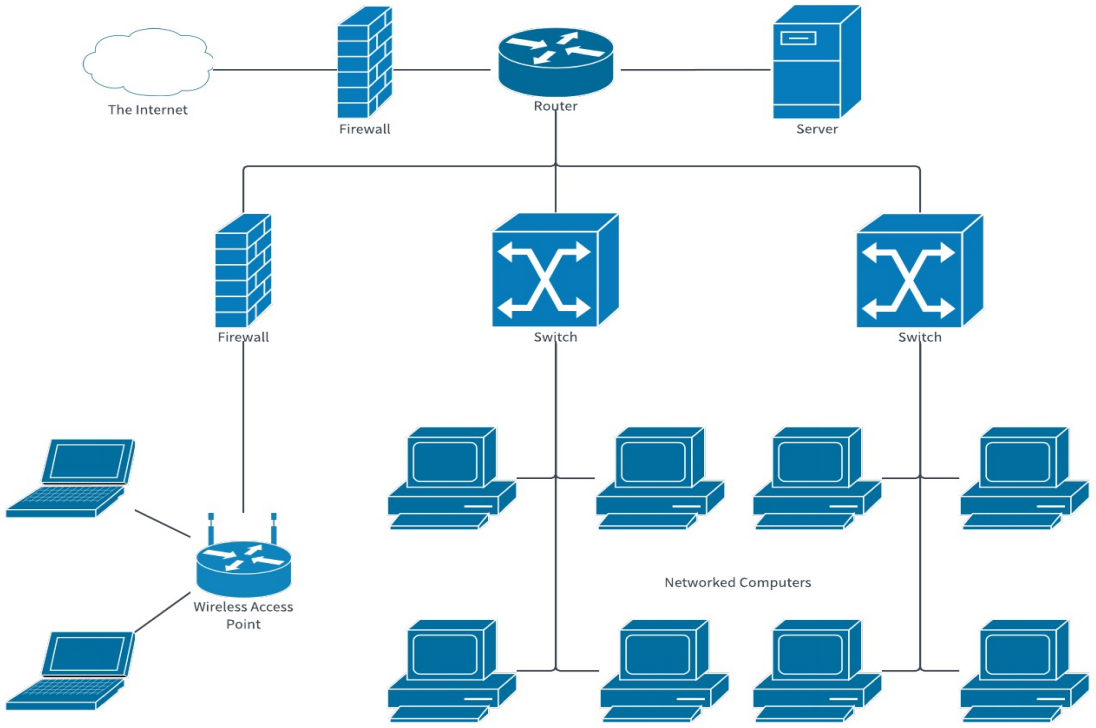
- No router can go faster than your Internet connection allows.
- Security (WEP, WPA, WPA2) *[Yes, I know!]*
  - Access controls
    - Multiple SSIDs
    - Guest Access
- Wired connectivity
- Single WAN or Dual-WAN

- Economic
- Talent
- Existing Equipment
-  Function

4 Points of Alignment

Credit: Kaspersky.com

Level 2

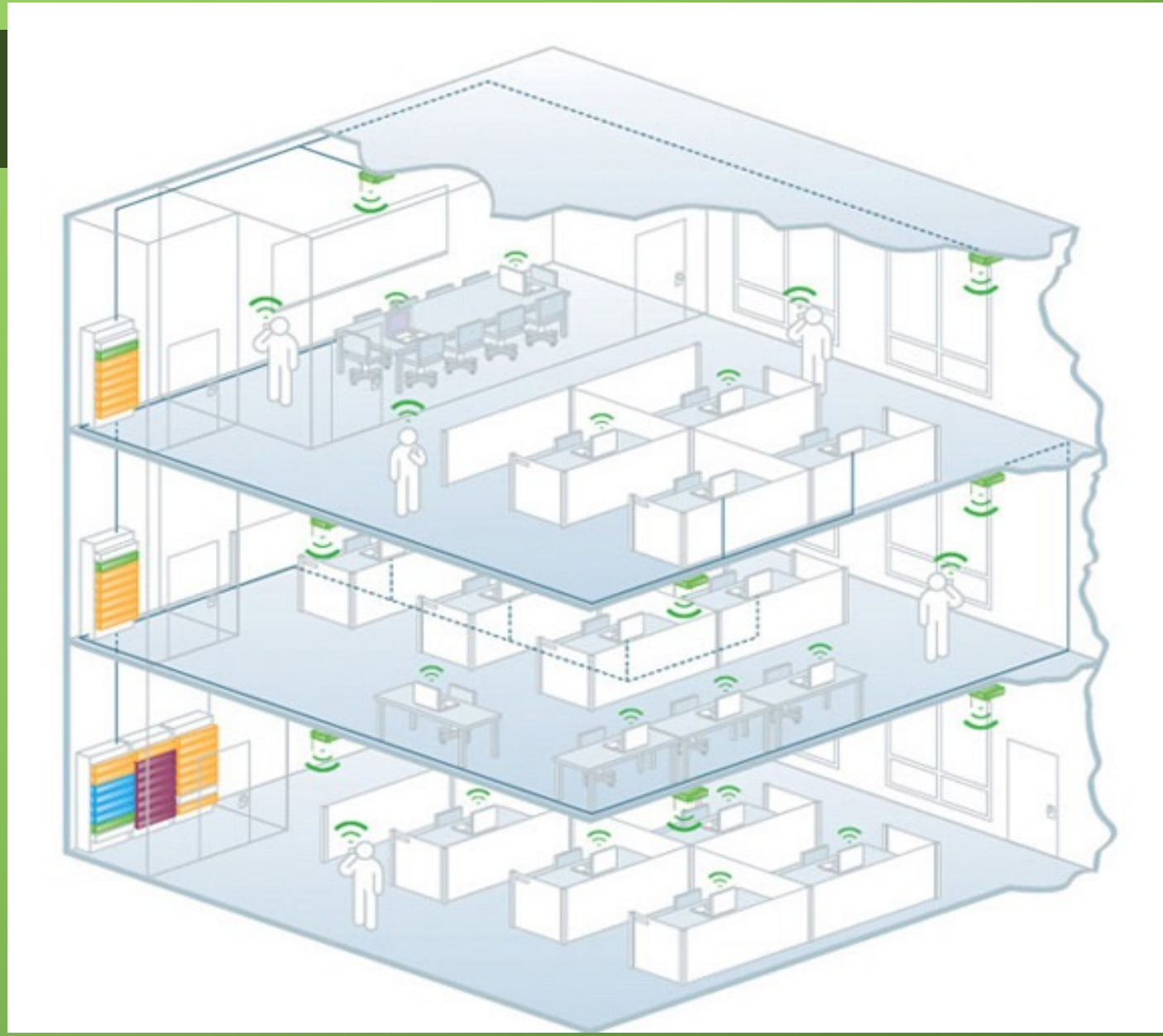

The Internet
Firewall
Router
Server
Firewall
Switch
Switch
Wireless Access Point
Networked Computers


S.O.P
TEAM WORK
Rp
HELP
PEOPLE
£
BRAND
Ideas
Inspiration
Confident
Leadership
Success
Motivation
Spirit
Communication
Teamwork
Smart
Innovation
Vision
Plan
SUCCESS

Level 3

Process standardization on best practices is evident

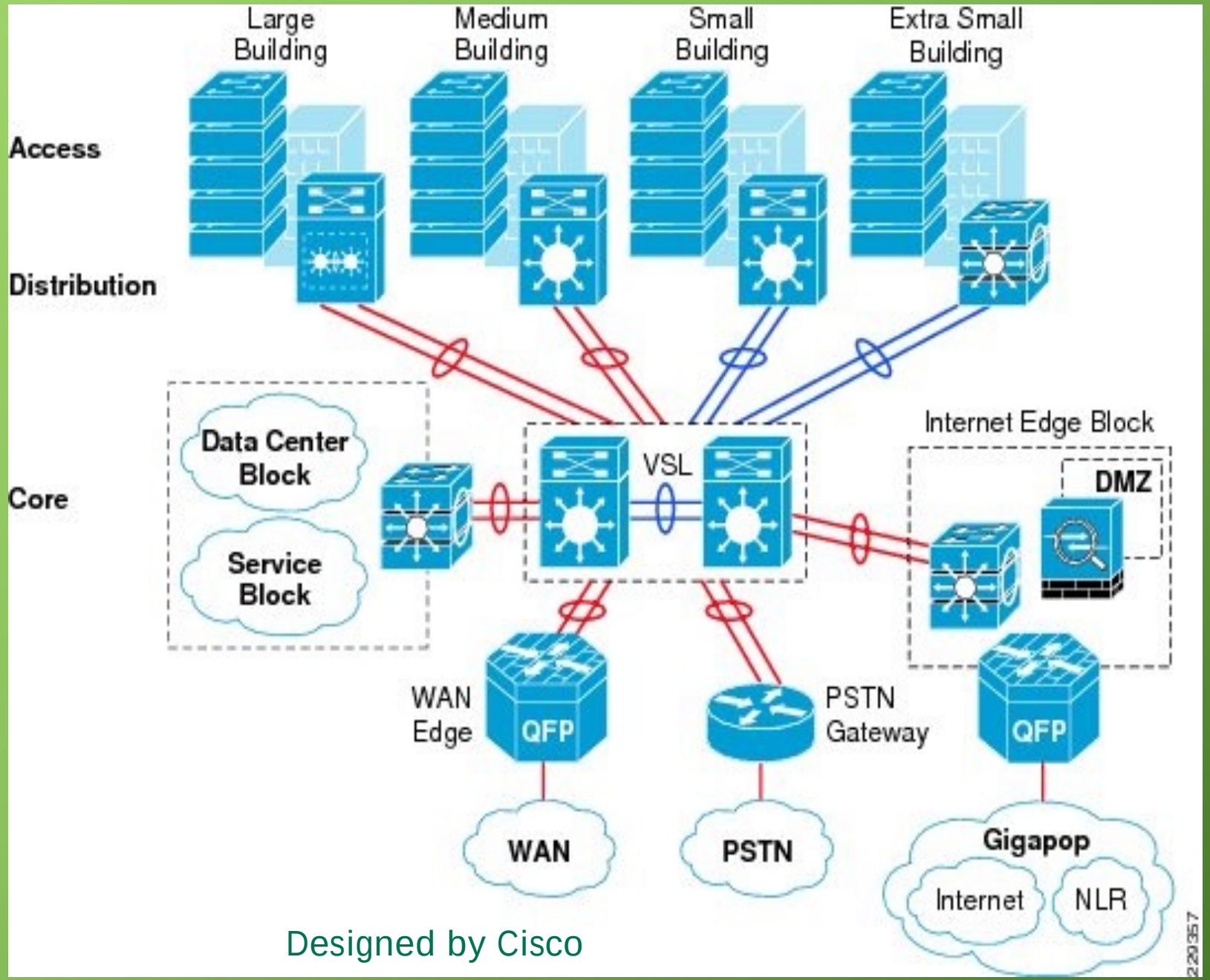
- Requirements Development
- Technical solutions
- Product integration
- Verification & Validation
- Process focus & definition
- Organizational Training
- Integrated Project Management
- Risk Management
- Decision Analysis and Resolution
- Comprehensive approach for managing change is being applied in multiple projects



Level 4

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

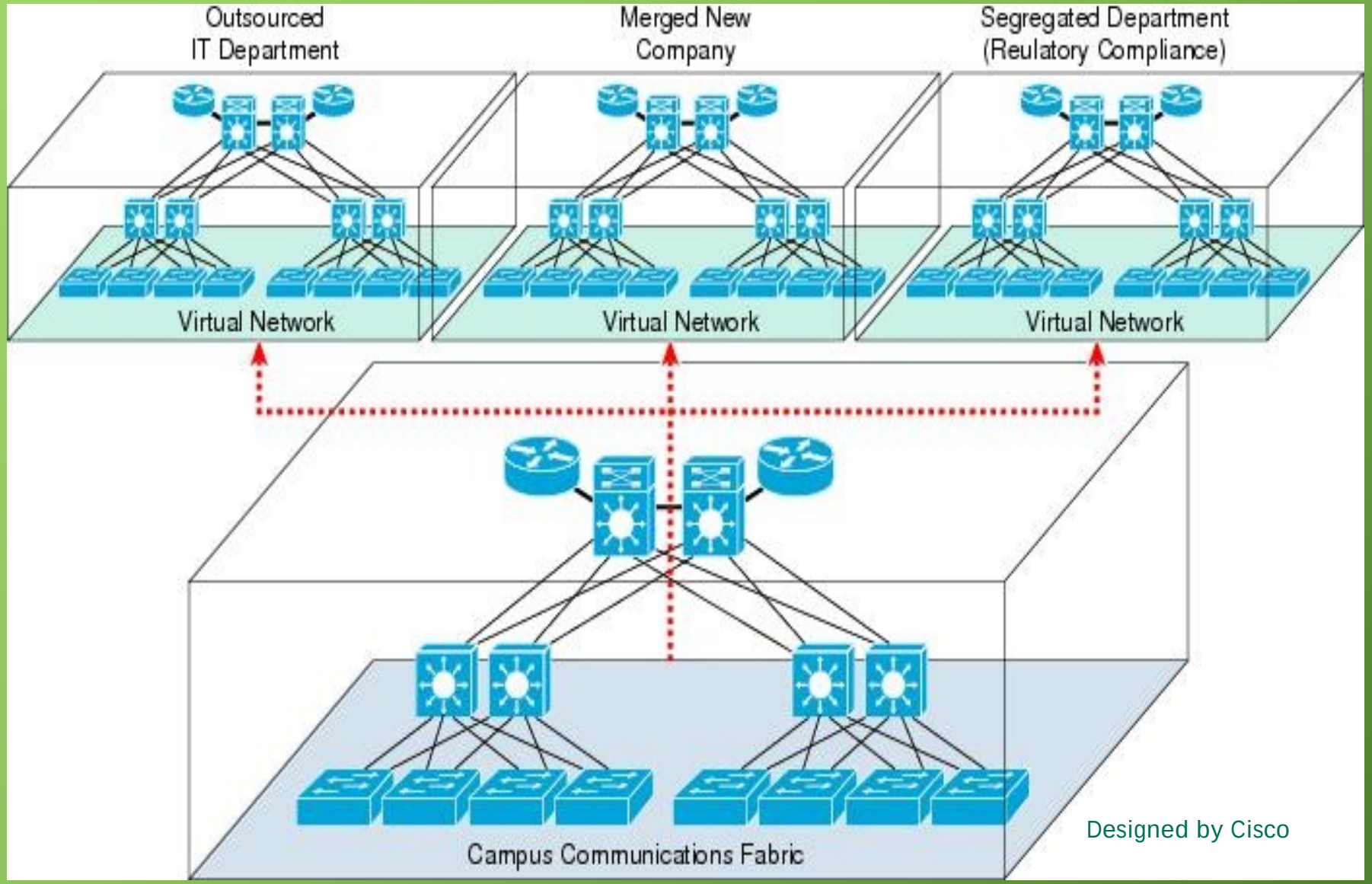


Designed by Cisco

Level 5

CPI is fully operationalized at the enterprise level

- Causal Analysis
- Change management in all levels of the organization and is part of the company's intellectual property and competitive edge.



Designed by Cisco

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

Board C-Level & Stakeholder Reporting

Reporting	Frequency
Board	Quarterly if not monthly
Committee of the Board	Quarterly if not monthly
CEO	Monthly & PRN
Senior Management Team	Monthly & PRN
Key Stakeholders	Monthly & PRN

Report Contents

Reporting	Frequency
Board	*Are we safe?* *Meaningful* metrics Budget performance Overall program status (program, policy, procedure, process,& projects)
Committee of the Board	Same as the Board
C-Suite	The Board + Threats & Vulnerabilities Patch Management Events, Incidents & Breaches
Key Stakeholders	All the above & line of business information

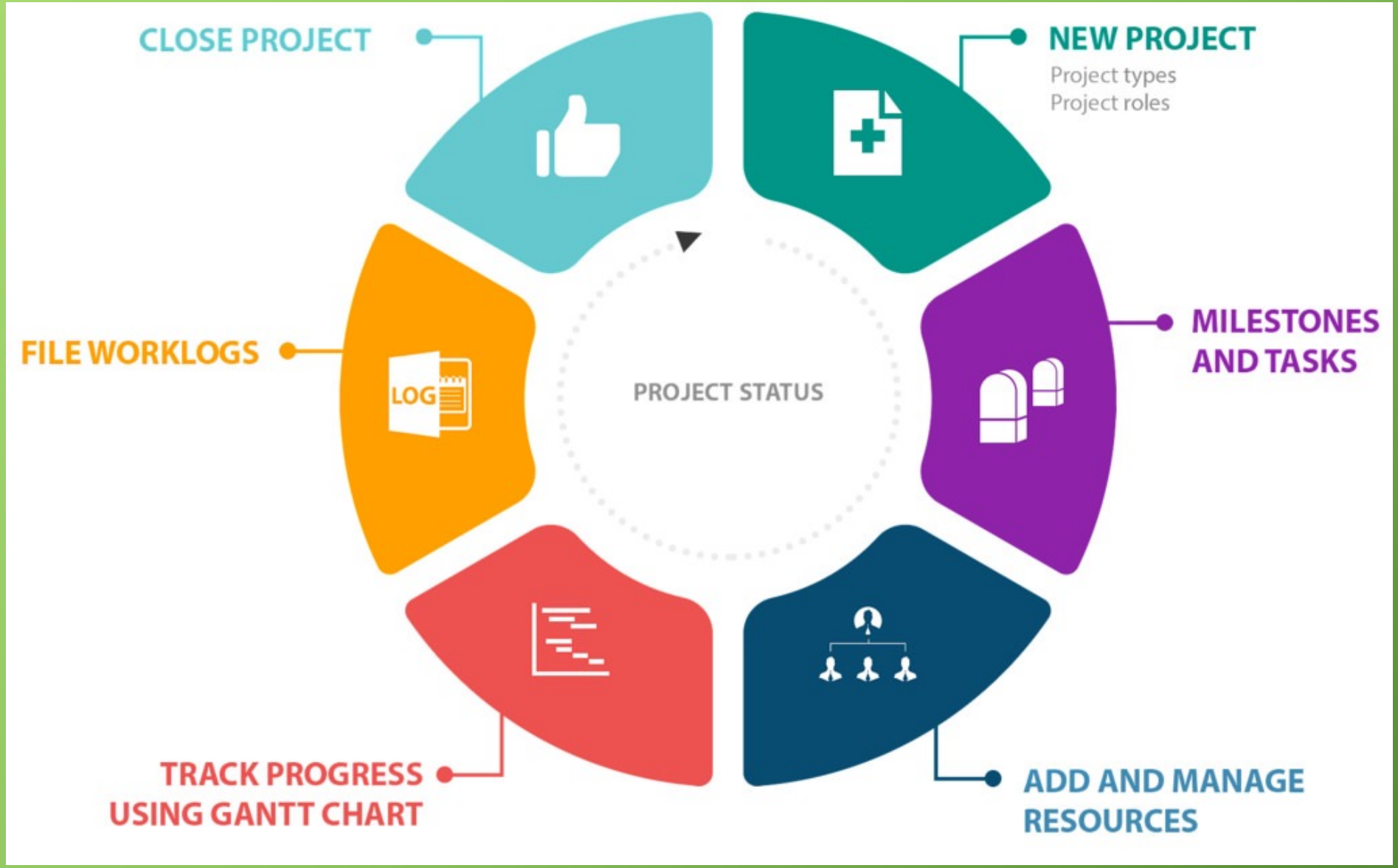
Risk Appetite Statement

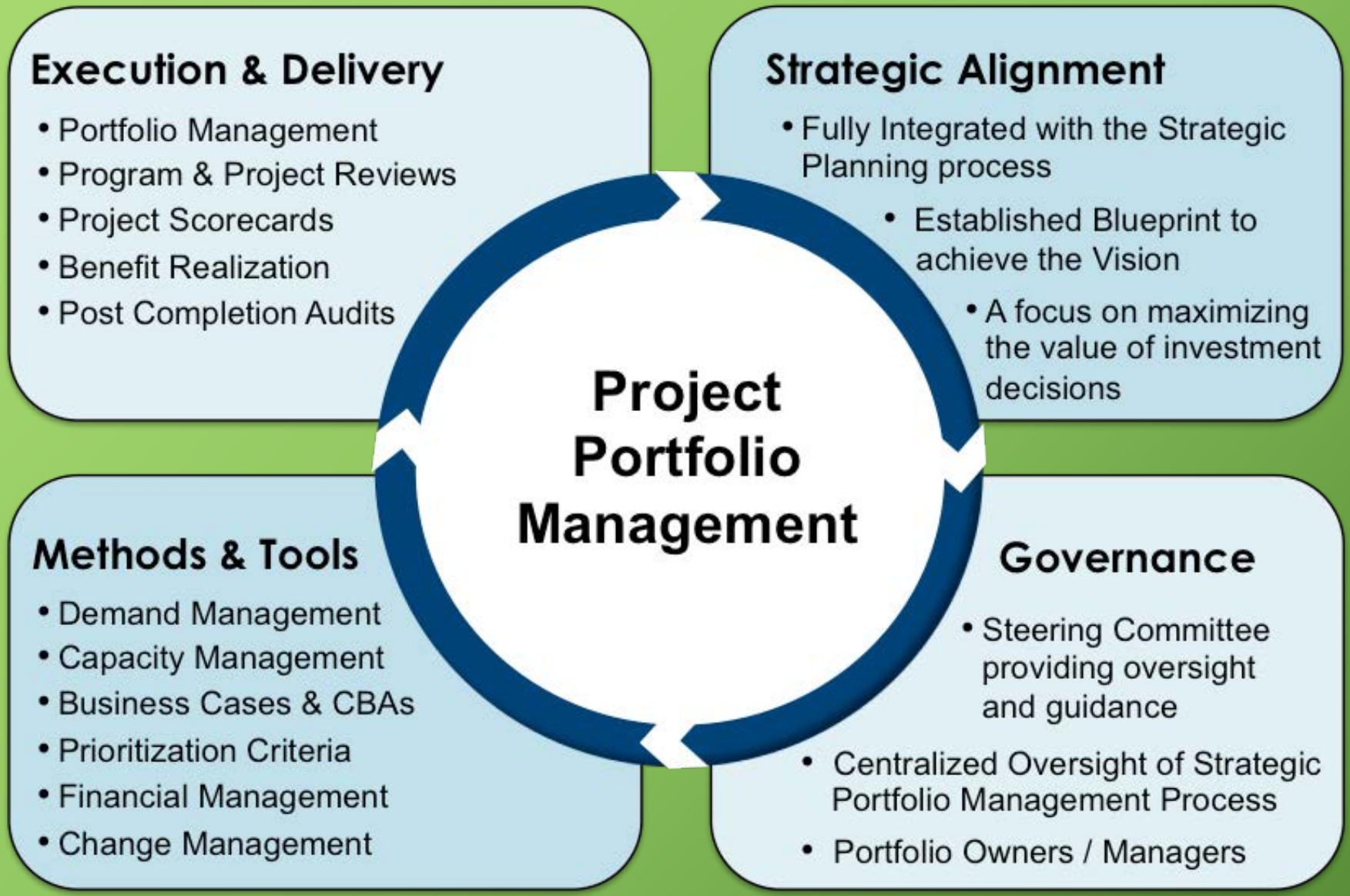
- What’s a material loss?
- Use a framework!
- There are many to choose from.
  - COSO Framework
  - NIST
  - ISO

ASSESS

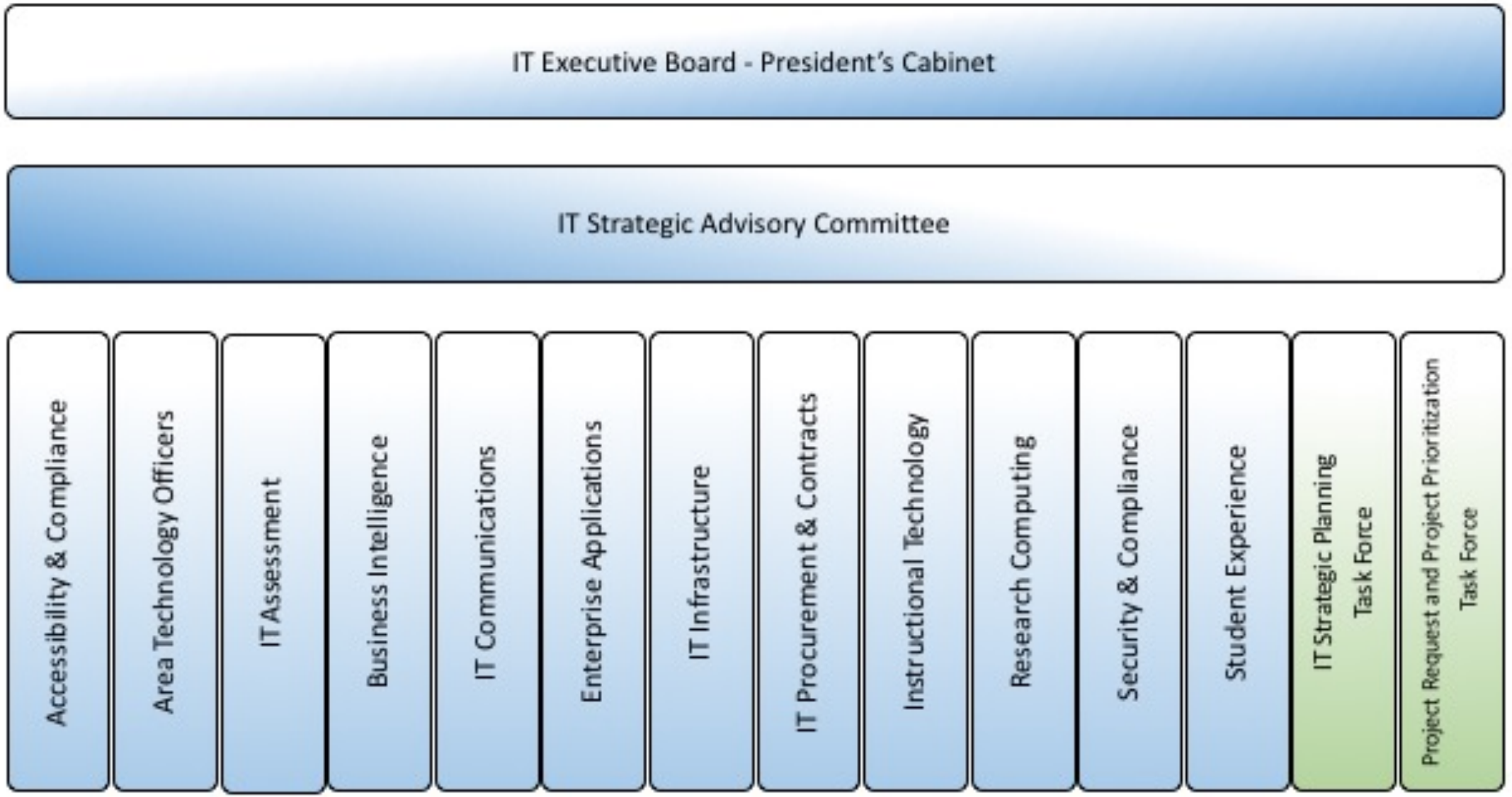
1. People | Processes | Technology
2. Talent level
3. Project management capability
4. Standardization
5. Quantitative management capability (Golden Circle)

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


CLOSE PROJECT
NEW PROJECT
Project types
Project roles
FILE WORKLOGS
LOG
PROJECT STATUS
MILESTONES
AND TASKS
TRACK PROGRESS
USING GANTT CHART
ADD AND MANAGE
RESOURCES


Execution & Delivery
• Portfolio Management
• Program & Project Reviews
• Project Scorecards
• Benefit Realization
• Post Completion Audits
Strategic Alignment
• Fully Integrated with the Strategic Planning process
• Established Blueprint to achieve the Vision
• A focus on maximizing the value of investment decisions
Project Portfolio Management
Methods & Tools
• Demand Management
• Capacity Management
• Business Cases & CBAs
• Prioritization Criteria
• Financial Management
• Change Management
Governance
• Steering Committee providing oversight and guidance
• Centralized Oversight of Strategic Portfolio Management Process
• Portfolio Owners / Managers

IT Governance



Frameworks

Framework	Best utilization
1. NIST CSF	1. Cybersecurity
2. CMM	2. Software Development
3. COSO	3. Enterprise Risk Management
4. COBIT	4. IT Governance/Controls
5. ITIL/ITSM	5. IT Service Management
6. ISO/IEC 27001	6. Cybersecurity
7. TOGAF	7. Enterprise Architecture
8. Zachman	8. 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
1. Risk Assessments	1. Annually and PRN
2. Code reviews	2. Development - team sport
3. Patches	3. Weekly and PRN
4. System Configuration	4. 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 Successful CISOs Excel

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

Gordon Rudd
Tech Career Designer | Executive Coach
Stone Creek Coaching
(918) 640-5706
gordon@stonecreekcoaching.com