

Bond University  
Research Repository



## Shields Up: Cybersecurity Project Management

Skulmoski, Gregory James

*Published in:*  
PMI Webinar

*Licence:*  
CC BY-NC-ND

[Link to output in Bond University research repository.](#)

*Recommended citation(APA):*  
Skulmoski, G. J. (2022). Shields Up: Cybersecurity Project Management. *PMI Webinar*.  
<https://youtu.be/GDqMnlBetkY>

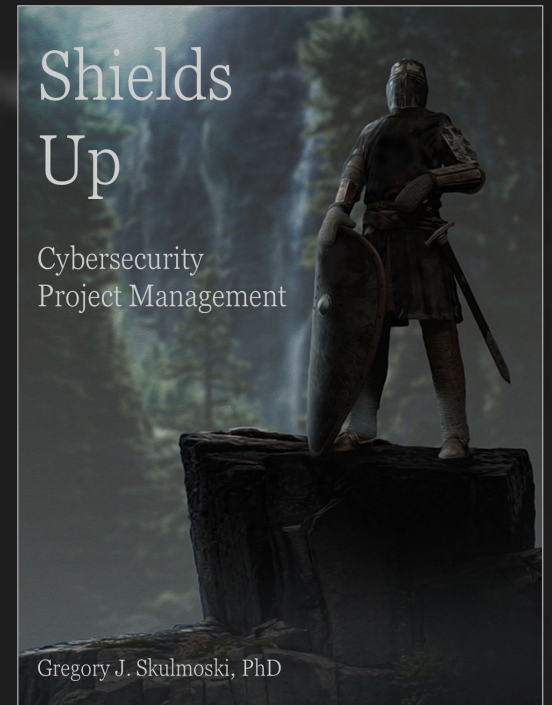
### **General rights**

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

For more information, or if you believe that this document breaches copyright, please contact the Bond University research repository coordinator.

# Cybersecurity Project Management

Greg Skulmoski PhD, MBA, BEd, CITP, FBCS  
Associate Professor, Project Management  
Faculty of Society and Design



“Best I Have Seen In My Career”

Some of your explanations of familiar topics and tools are among the best I have seen in my career.

Distinguished Professor Emeritus Timothy Kloppenborg PhD  
Project Management, Xavier University, United States

# Three Key Points

1

Cybersecurity is  
risk management

2

Project delivery  
underpins cybersecurity

3

Front-end-load to shift the  
information curve

# Biography: Dual Careers



1990s  
Challenged Technology  
Projects



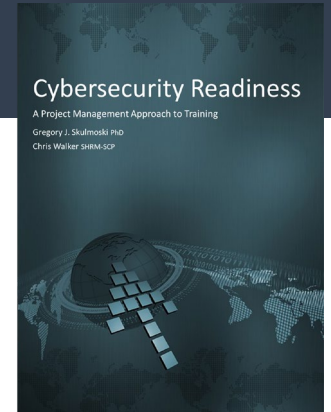
2007  
Top IT Teacher Award  
Zayed University



2017  
CISO Rising Star

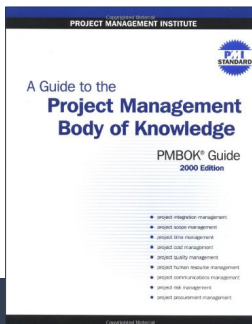


2021  
Top 10 Medical Innovations  
Cleveland Clinic



2023  
*Cybersecurity Readiness: A  
Project Management Approach  
to Training*

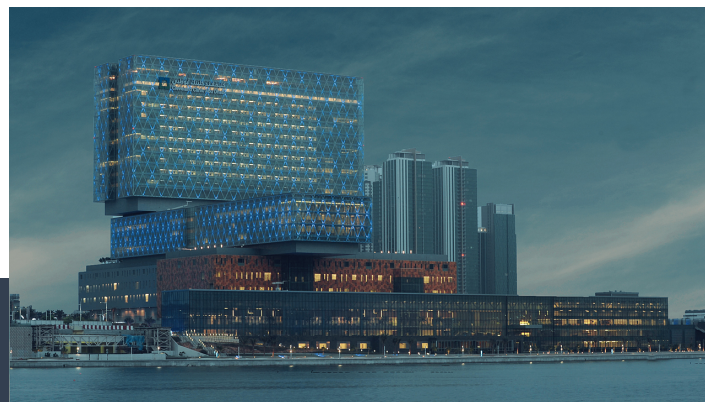
2000  
PMBOK Guide  
"Author"



2004  
PhD  
Project Management



2011  
Project Manager  
Cleveland Clinic Abu Dhabi



2018  
Project Innovation Management



2022 August  
*Shields Up: Cybersecurity  
Project Management*



## Outline

1. **High Demand** for Cybersecurity Projects
2. **Align Standards for** Cybersecurity Project Success
3. **Risk Management** Strategy Not in the PMBOK Guide



# What is Cybersecurity? Risk Management!

kaspersky

## Defending digital assets from malicious attacks

### Cybercrime

Target systems for financial gain or to disrupt

### Cyber-attack

Politically motivated information gathering

### Cyberterrorism

Undermine digital systems to cause panic or fear

August 10, 2023

287 Days

to detect and contain a security breach

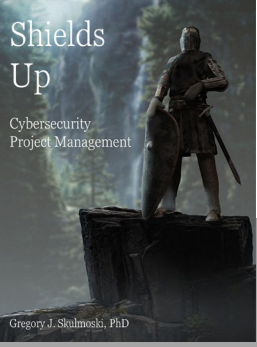
Identify Mitigate







# How Does Cybersecurity Work?



"NIST Cybersecurity Framework"



## Framework for Improving Critical Infrastructure Cybersecurity

Version 1.1

National Institute of Standards and Technology

April 16, 2018

- Agriculture
- Banking & Finance
- Communications
- Defence & Defence Industry
- Energy & Environment
- Health
- Transport & Logistics
- Education and Research
- Mining and Resources
- Manufacturing
- Space



55 pages



# Three Cybersecurity Project Drivers

More

1

## Digital Transformation

AI and Quantum Computing

More

2

## Cyber Attacks

Very Lucrative \$\$\$  
AI and Quantum Computing

More

3

## Compliance

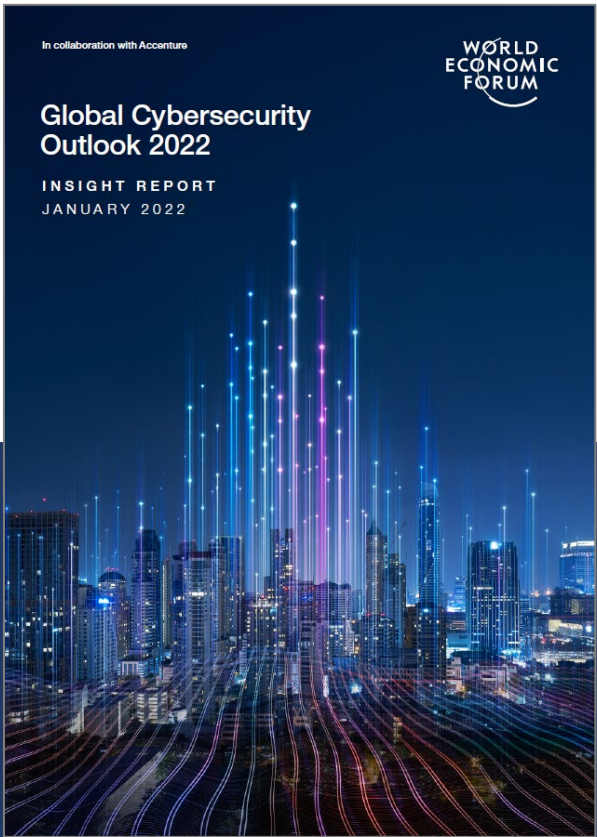
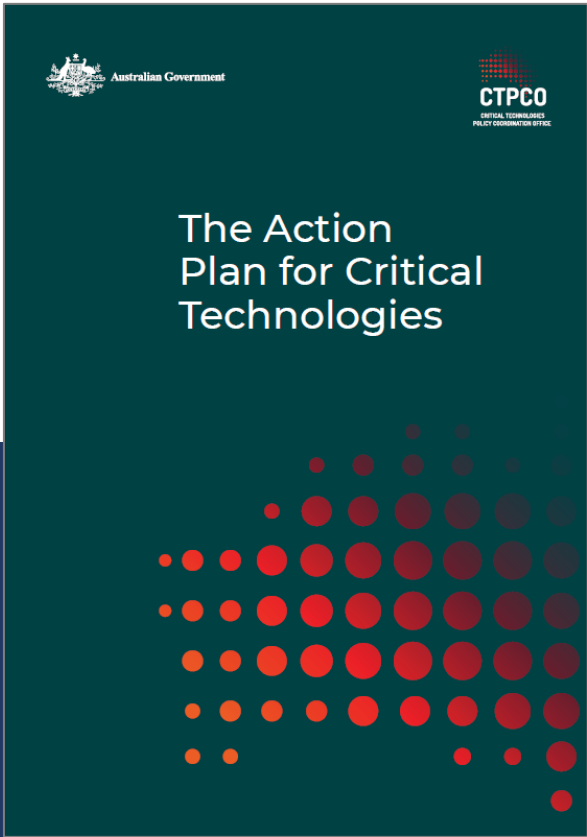
Regulations and Insurance

Result

Increase in Demand for **Cybersecurity Projects**  
and **Cybersecurity Project Managers**

Supply  
"Crisis!"





# strong demand for cybersecurity

and cybersecurity projects and project managers!!!!



# CYBER ATTACK TRENDS

Check Point's 2022 Mid-Year Report



262,000  
“Hacktivists”

Ukrainian Minister of Digital Transformation, Is calling for “digital talents” to join their IT army. (p. 11)



“The threat from **state-sponsored** cybercrime is now so serious, it is no exaggeration to say that it is time for enterprises to put their entire security teams on a **war footing.**”



Microsoft Digital Defense Report 2021

Advanced materials and manufacturing



AI, computing and communications



Biotechnology, gene technology and vaccines



Energy and environment



Quantum



Sensing, timing and navigation



Transportation, robotics and space



“Protective Cybersecurity Technologies”

Implemented

Optimized

Protected

Through  
Projects



Australian Government



# The Action Plan for Critical Technologies





# DEFENCE CYBER SECURITY STRATEGY



“Defence adopts leading cyber security **standards** that strengthen its cyber security posture.” (p. 11)

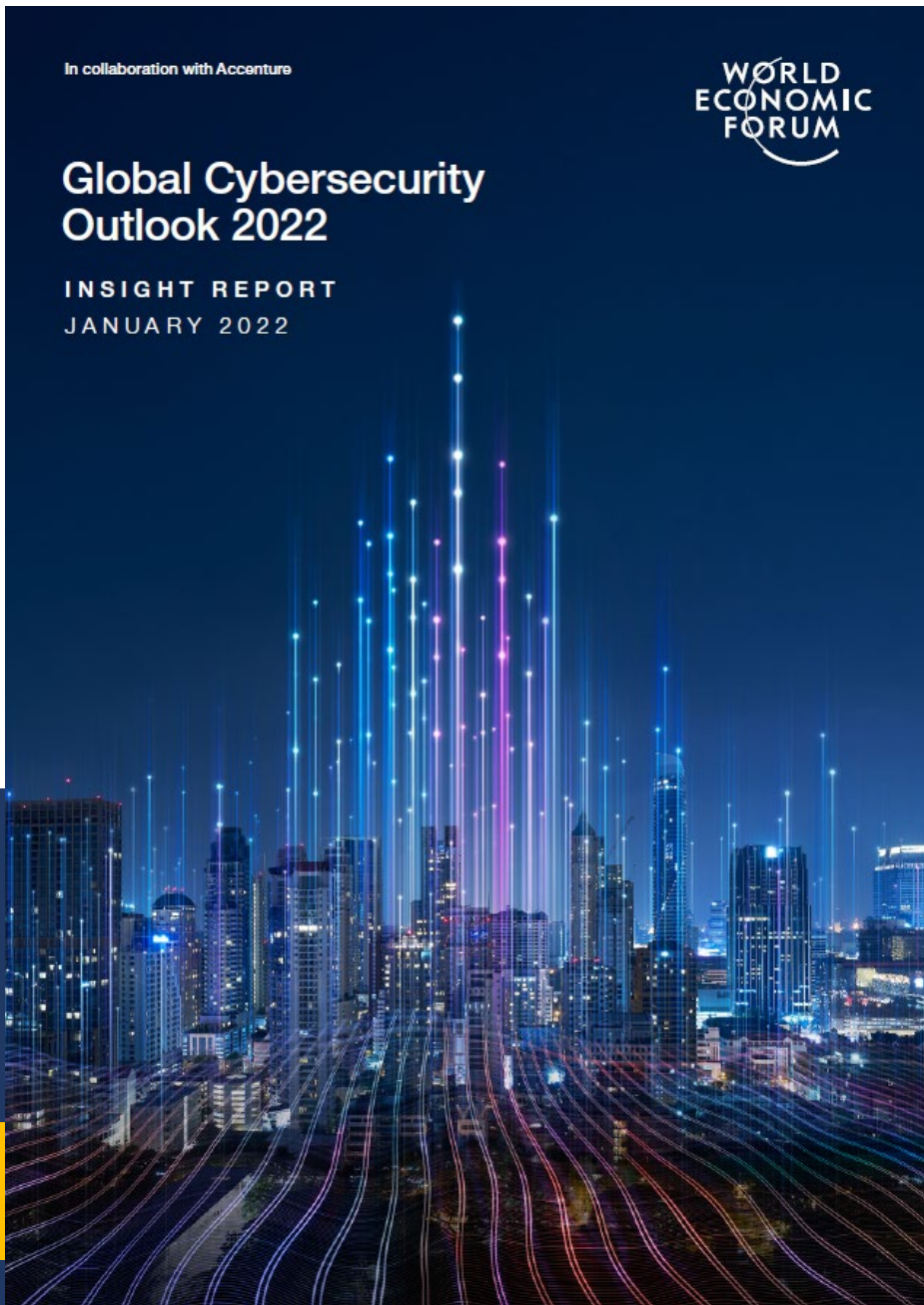


**ISO 27001**  
Information Security Management

**NLST**



“Defence must continue to improve its cyber security if it is to defend against **constant and malicious cyber activity** and **succeed in future conflicts.**”

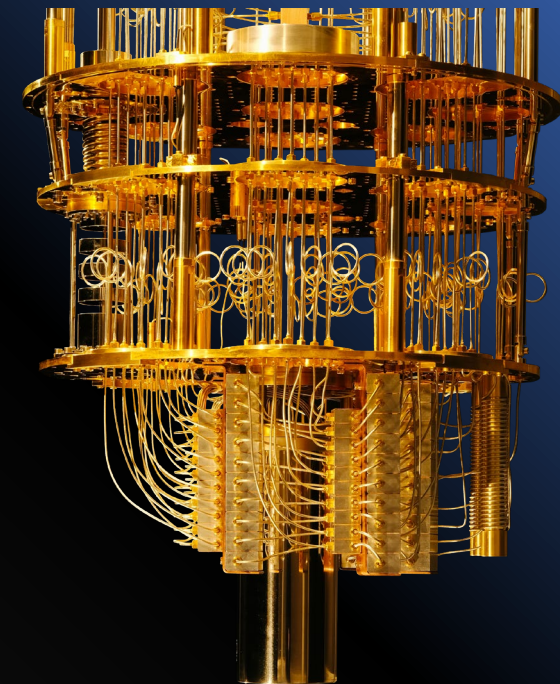


In collaboration with Accenture

WORLD  
ECONOMIC  
FORUM

# Global Cybersecurity Outlook 2022

INSIGHT REPORT  
JANUARY 2022



## Hacking with Quantum Computer Technologies

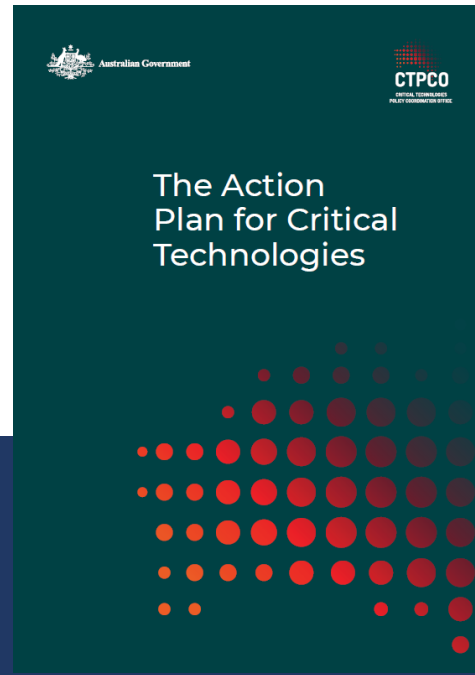
*At this stage of mass digitalization, it is imperative that leadership prepare for potential **cyber disasters**.* (p. 29)

**Status: "Cyber Arms Race"**





Recommendation:  
War Footing



Cybersecurity is a  
Critical Technology



Cybersecurity is a  
National Security Priority



Prepare for Quantum  
Cybersecurity Threats





# Cybersecurity Project Management

What's the Best Project Management Approach?

What Standards Should We Follow? How?



ISO 31000  
Risk Management



ISO 9001  
Quality Management

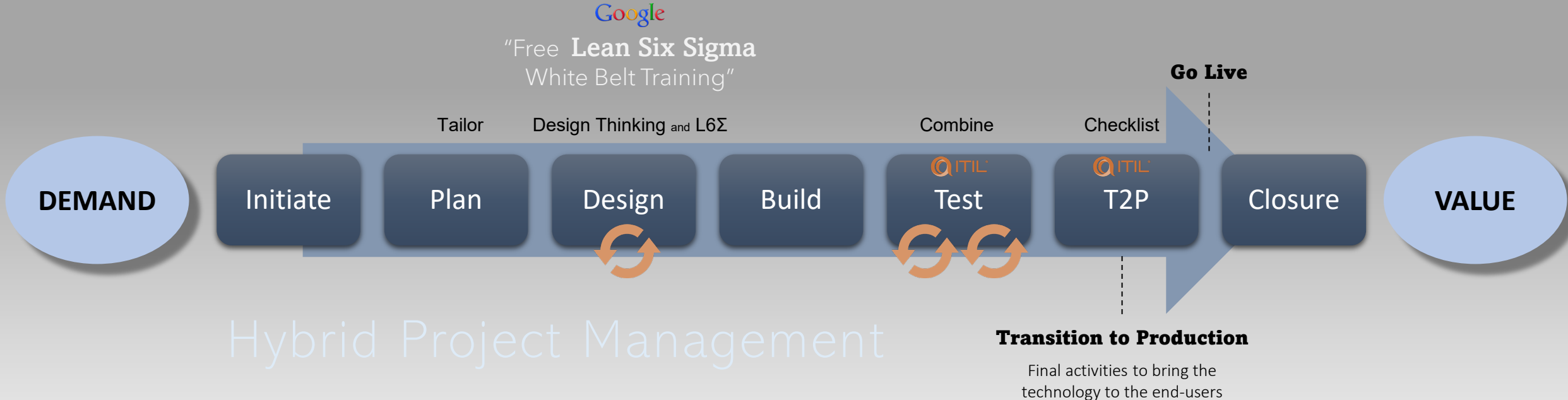
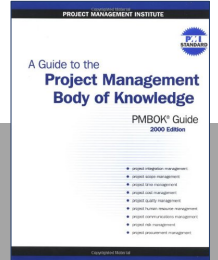
NIST



ISO 27001  
Information Security  
Management

# What's the "Best" Project Management Approach?

This is Project Management Applied to Cybersecurity Projects  
"Most [cybersecurity] projects, most of the time"



## Value Proposition

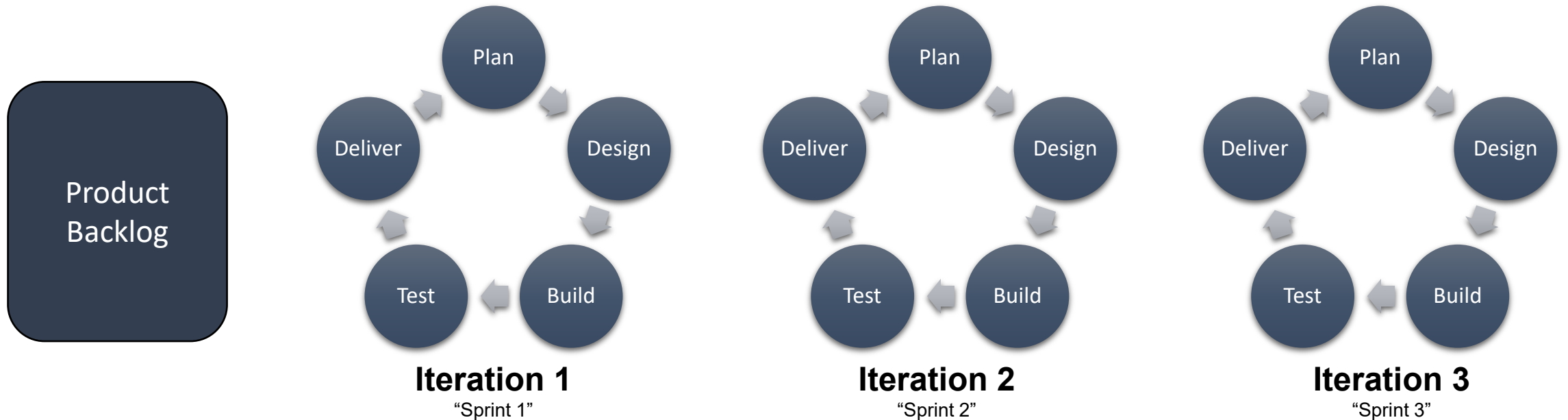
Follow the project management approach to keep quality high and risks low



# What About Agile Project Management?



## Continual Improvement



### Value Proposition

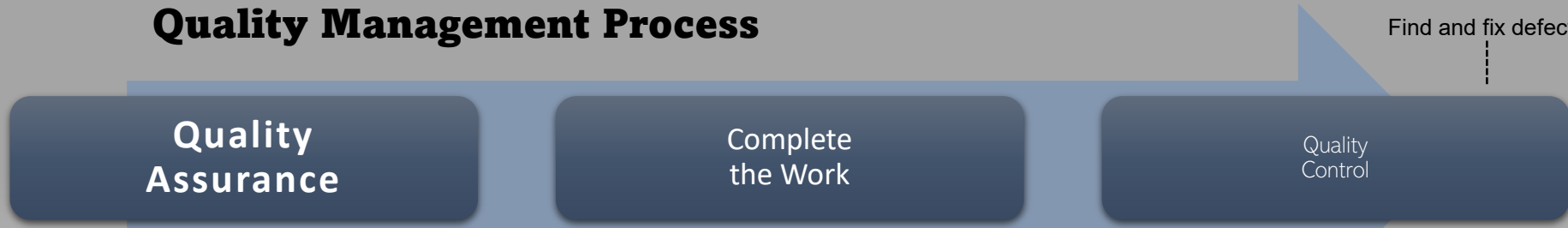
Follow the Agile project management approach to keep quality high and risks low

# Best Project Management Approach

## Prioritize Quality Management



### Quality Management Process



**Quality Assurance**

**Complete the Work**

**Quality Control**

Find and fix defects

**A**ssurance

**B**efore

**C**ontrol

**Achieve QA With:**

- Training
- Processes
- Templates / Checklists

**Project Plan**

**Build** a house

**Create** a website

**Install** an elevator system

**Recruit** the project manager

**Rectify** the contaminated site

**Implement** a pharmacy system

**Test** organosilicon electrolyte batteries

**Achieve QC With:**

- Processes
- Checklists
- Stage Gates



### Value Proposition

Follow the quality management approach to keep quality high and risks low



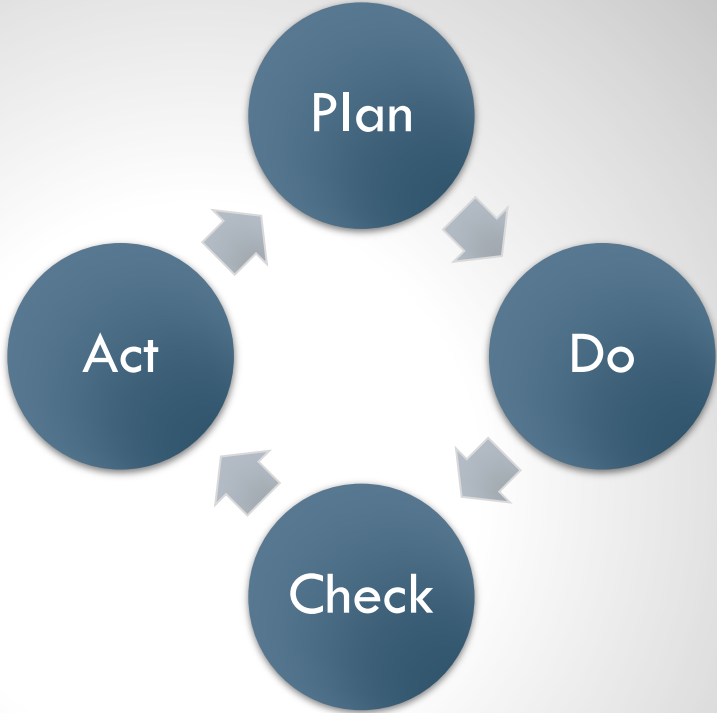
**ISO 9001**  
**Quality Management**

# Continual Improvement

Used in  
Cybersecurity  
Projects ...

## Deming Cycle

Classical Quality Management Theory



Ed Deming

*“Leadership is only 99%  
of the problem”*



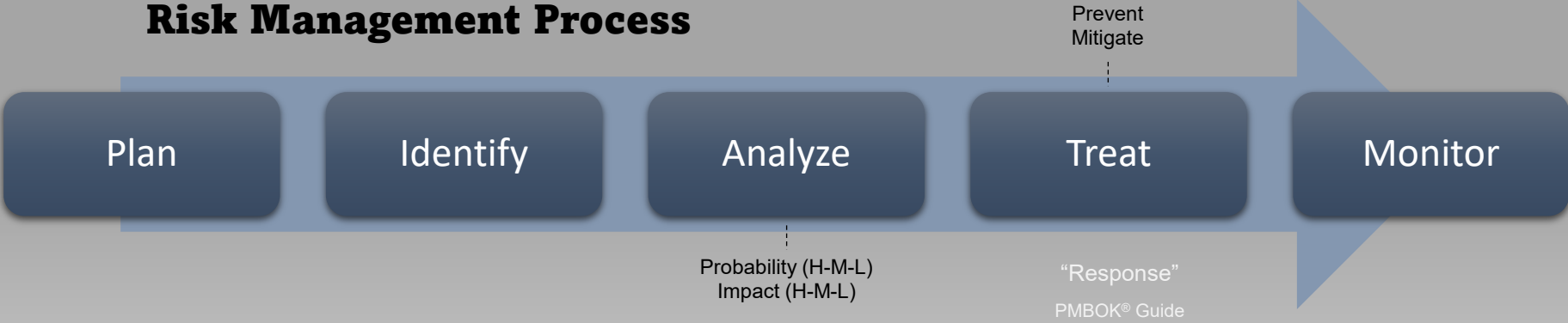
ISO 9001  
Quality Management





# Best Project Management Approach

## Include Risk Management



### Value Proposition

Follow the risk management approach to keep quality high and risks low



ISO 31000  
Risk Management





# Best Project Management Approach

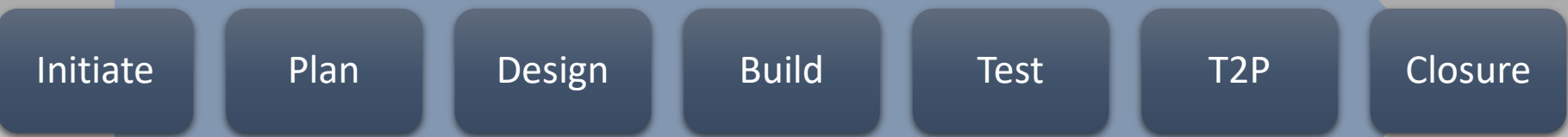
# Incorporate Standards



Same-Same in Cybersecurity Projects!

Integration Management (Tailor and Combine → Hybrid Project Management)

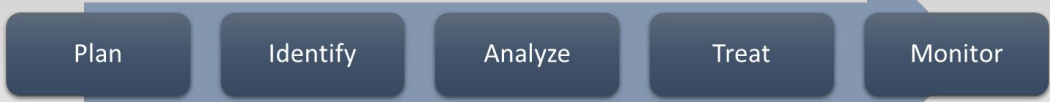
## Project Management Delivery Approach



### Quality Management



### Risk Management



Quality and Risk Management are Best Practices in Project Management

# ITIL Service Management

A framework to guide organizations to deliver digital services



ITIL "Service Value System"

Demand  
or  
Opportunity

Project Delivery  
"Service Value Chain"

Initiate Plan Design Build Test T2P Closure

Operations

Provide Value

Continual  
Improvement

Strategy Management

Project Management

Risk Management

Release Management



ISO 31000  
Risk Management

Service Desk  
Incident Management

Service Request  
Management

Continual Improvement



ISO 9001  
Quality Management

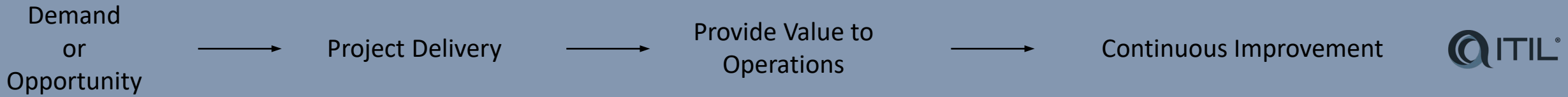
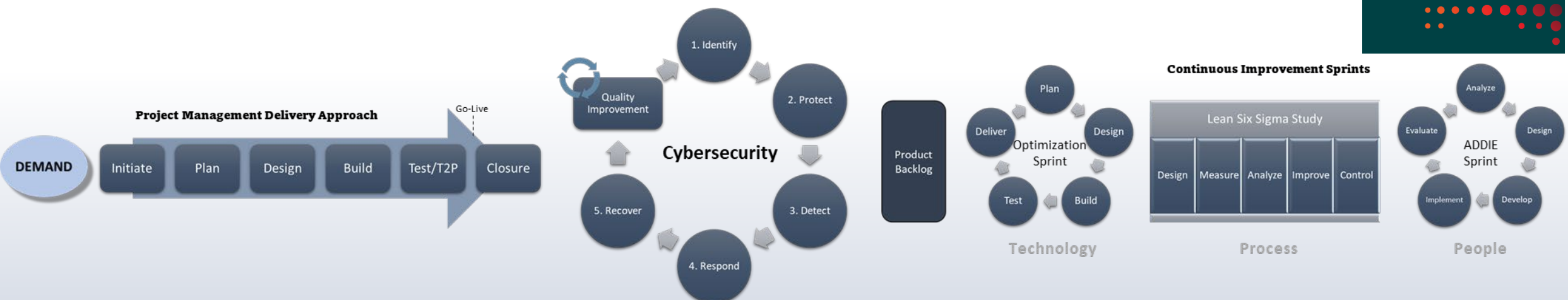


ITIL has 34 practices (vs 10 Knowledge Areas\*)

Incorporate Standards

# Best Project Management Approach for Digital Requirements

Integration Management / Combining / Tailoring

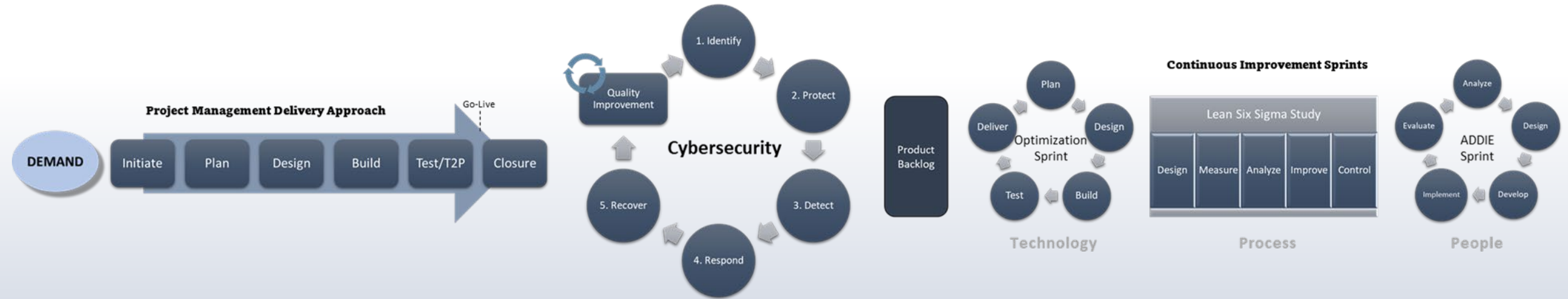


Service, Project, Quality and Risk Management Standards Alignment



# Best Digital Project Management Approach Incorporate Standards

Integration Management / Combining / Tailoring



Demand  
or  
Opportunity



Project Delivery



Provide Value to  
Operations



Continuous Improvement



Apply this integrated approach to **cybersecurity** project management

## 3 Use Cases

# Cybersecurity Project Management



Use Case #1 Implement Cybersecurity Software

**Implement** SOAR (Security Orchestration, Automation and Response) **software** v2.3

Project Rationale: Improve detection and response capabilities

# Cybersecurity **IN** Technology Projects

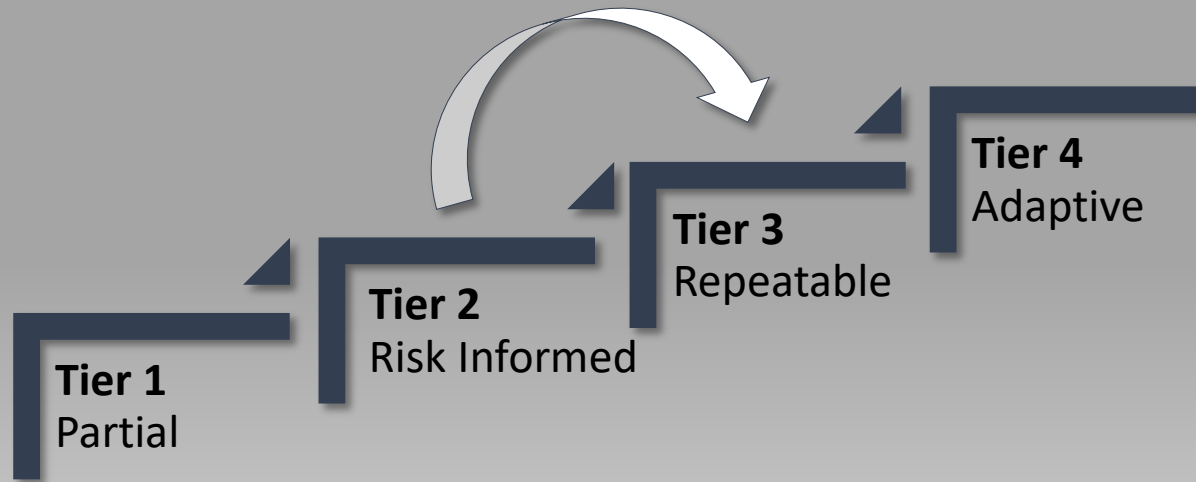


Use Case #2 Design-in Cybersecurity

Implement technology (e.g., industrial automation) and “design-in” security



# NIST Cybersecurity Tiers



## Key Points

- ✓ Plan and improve cybersecurity capabilities
- ✓ Demonstrate cybersecurity maturity

Use Case #3

**Conduct** a cybersecurity internal **audit**

**LOW** Complexity Project

Clear Requirements - NIST  
No Testing  
Follow the Audit Process

# CYBERSECURITY AUDIT

# 5 NIST CYBERSECURITY FUNCTIONS



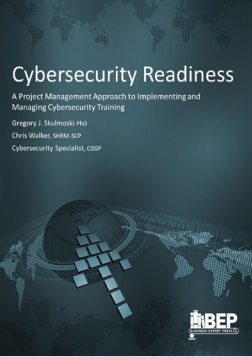
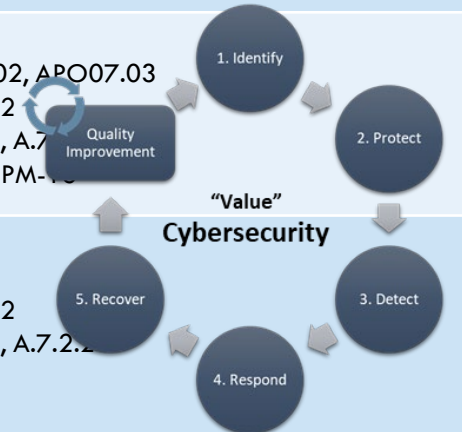
Identify One	Protect Two	Detect Three	Respond Four	Recover Five
<ul style="list-style-type: none"> <li>Asset Management</li> <li>Business Environment</li> <li>Governance</li> <li>Risk Assessment</li> <li>Risk Management Strategy</li> </ul>	<ul style="list-style-type: none"> <li>Access Control</li> <li>Awareness and Training</li> <li>Data Security</li> <li>Information Protection</li> <li>Maintenance</li> <li>Protective Technology</li> </ul>	<ul style="list-style-type: none"> <li>Anomalies and Events</li> <li>Security Continuous monitoring</li> <li>Detection Processes</li> </ul>	<ul style="list-style-type: none"> <li>Response Planning</li> <li>Communications</li> <li>Analysis</li> <li>Mitigation</li> <li>Improvements</li> </ul>	<ul style="list-style-type: none"> <li>Recovery Planning</li> <li>Improvements</li> <li>Communications</li> </ul>

Function	Category	Subcategory	References
Protect (PR)	<b>Awareness and Training (PR.AT)</b> The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	<b>PR.AT-1</b> All users are informed and trained	CIS CSC 17, 18 COBIT 5 APO07.03, BAI05.07 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.7.2.2, A.12.2.1 NIST SP 800-53 Rev. 4 AT-2, PM-13
		<b>PR.AT-2</b> Privileged users understand their roles and responsibilities	CIS CSC 5, 17, 18 COBIT 5 APO07.02, DSS05.04, DSS06.03 ISA 62443-2-1:2009 4.3.2.4.2, 4.3.2.4.3 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 NIST SP 800-53 Rev. 4 AT-3, PM-13
		<b>PR.AT-3</b> Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities	CIS CSC 17 COBIT 5 APO07.03, APO07.06, APO10.04, APO10.05 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.7.2.2 NIST SP 800-53 Rev. 4 PS-7, SA-9, SA-16
		<b>PR.AT-4</b> Senior executives understand their roles and responsibilities	CIS CSC 17, 19 COBIT 5 EDM01.01, APO01.02, APO07.03 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 NIST SP 800-53 Rev. 4 AT-3, PM-13
		<b>PR.AT-5</b> Physical and cybersecurity personnel understand their roles and responsibilities	CIS CSC 17 COBIT 5 APO07.03 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2

## Awareness and Training Category

IMPLEMENTED THROUGH PROJECTS

# INTENDED OUTCOMES BY CATEGORY AND SUBCATEGORY

Function	Category	Subcategory	References
<p><b>Protect (PR)</b></p> 	<p><b>Awareness and Training (PR.AT)</b>            The organization’s personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.</p>	<p><b>PR.AT-1</b>            All users are informed and trained</p> <p><b>PR.AT-2</b>            Privileged users understand their roles and responsibilities</p> <p><b>PR.AT-3</b>            Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities</p> <p><b>PR.AT-4</b>            Senior executives understand their roles and responsibilities</p> <p><b>PR.AT-5</b>            Physical and cybersecurity personnel understand their roles and responsibilities</p> <p style="text-align: center;"><b>R e a d i n e s s</b></p>	<p>CIS CSC 17, 18            COBIT 5 APO07.03, BAI05.07            ISA 62443-2-1:2009 4.3.2.4.2            ISO/IEC 27001:2013 A.7.2.2, A.12.2.1            NIST SP 800-53 Rev. 4 AT-2, PM-13</p> <p>CIS CSC 5, 17, 18            COBIT 5 APO07.02, DSS05.04, DSS06.03            ISA 62443-2-1:2009 4.3.2.4.2, 4.3.2.4.3            ISO/IEC 27001:2013 A.6.1.1, A.7.2.2            NIST SP 800-53 Rev. 4 AT-3, PM-13</p> <p>CIS CSC 17            COBIT 5 APO07.03, APO07.06, APO10.04, APO10.05            ISA 62443-2-1:2009 4.3.2.4.2            ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.7.2.2            NIST SP 800-53 Rev. 4 PS-7, SA-9, SA-16</p> <p>CIS CSC 17, 19            COBIT 5 EDM01.01, APO01.02, APO07.03            ISA 62443-2-1:2009 4.3.2.4.2            ISO/IEC 27001:2013 A.6.1.1, A.7.2.2            NIST SP 800-53 Rev. 4 AT-3, PM-13</p> <p>CIS CSC 17            COBIT 5 APO07.03            ISA 62443-2-1:2009 4.3.2.4.2            ISO/IEC 27001:2013 A.6.1.1, A.7.2.2</p> 

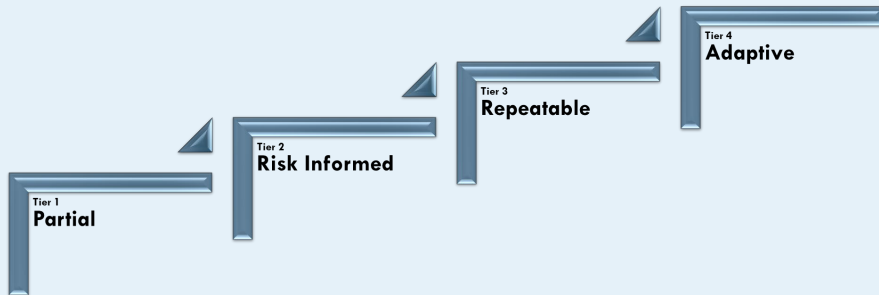
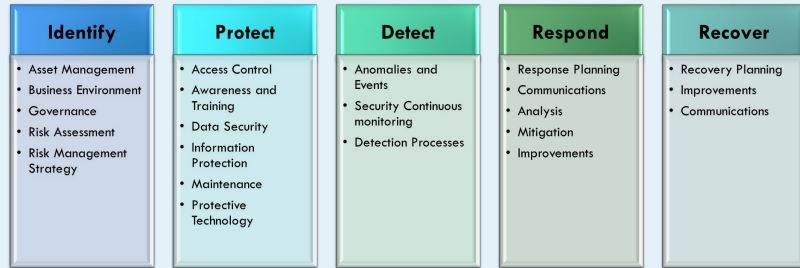
Auditors assess each **category** and **subcategory**, and document evidence

# CYBERSECURITY IMPROVEMENT PROCESS



Auditing Steps	Description
<b>Step 1: Prioritize and Scope</b>	Identify the business objectives and priorities to make cybersecurity decisions about the scope of the cybersecurity program
<b>Step 2: Orient</b>	Identify systems and assets, regulatory frameworks and overall risk approach, then identify related vulnerabilities and threats
<b>Step 3: Create a <b>Current</b> Profile</b>	Identify the functions, categories and subcategories being achieved
<b>Step 4: Conduct a Risk Assessment</b>	Assess the organisation against the framework noting compliance evidence
<b>Step 5: Create a <b>Target</b> Profile</b>	Create a target profile of where the organisation's cybersecurity program desired outcome
<b>Step 6: Determine, Analyse, and Prioritize <b>Gaps</b></b>	Determine, analyse and prioritise any cybersecurity gaps
<b>Step 7: Implement <b>Action Plan (project)</b></b>	Develop a plan to address any gaps. Some gaps will require more formal projects.

# NIST CYBERSECURITY FRAMEWORK



Function	Category	Subcategory	References
Protect (PR)	Awareness and Training (PR.AT) The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-1 All users are informed and trained	CS CSC 17, 18 COBIT 5 APO07.03, BA05.07 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.7.2.2, A.12.2.1 NIST SP 800-53 Rev. 4 A1-2, PM-13
		PR.AT-2 Privileged users understand their roles and responsibilities	CS CSC 5, 17, 18 COBIT 5 APO07.02, DS05.04, DS06.03 ISA 62443-2-1:2009 4.3.2.4.2, 4.3.2.4.3 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 NIST SP 800-53 Rev. 4 A1-3, PM-13
		PR.AT-3 Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities	CS CSC 17 COBIT 5 APO07.03, APO07.06, APO10.04, APO10.05 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.7.2.2 NIST SP 800-53 Rev. 4 PR7, SA-9, SA-16
		PR.AT-4 Senior executives understand their roles and responsibilities	CS CSC 17, 19 COBIT 5 EDM01.01, APO01.02, APO07.03 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 NIST SP 800-53 Rev. 4 A1-3, PM-13
		PR.AT-5 Physical and cybersecurity personnel understand their roles and responsibilities	CS CSC 17 COBIT 5 APO07.03 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2



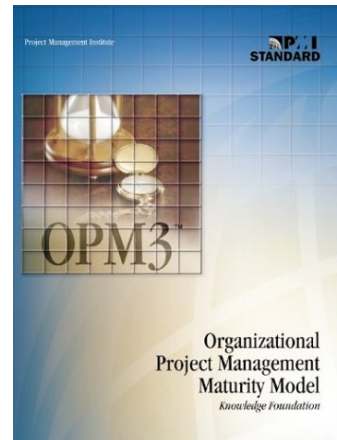
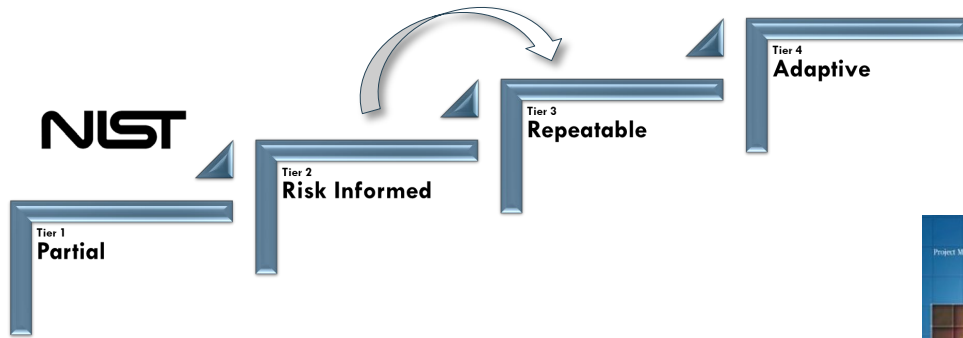
Gap Analysis



Prioritised Cybersecurity Initiatives and Projects

**NIST** Compliance = More Cybersecurity Projects

# QUALITY IMPROVEMENT THROUGH MATURITY



## Value Proposition

Follow the project management maturity approach to keep quality high and risks low

Domains	Standardize	Measure	Control	Improve
Portfolio				
Program				
Project				

Increasing Maturity

## Organizational Project Management Maturity Model (OPM3)

Guidance Committee Member 1999

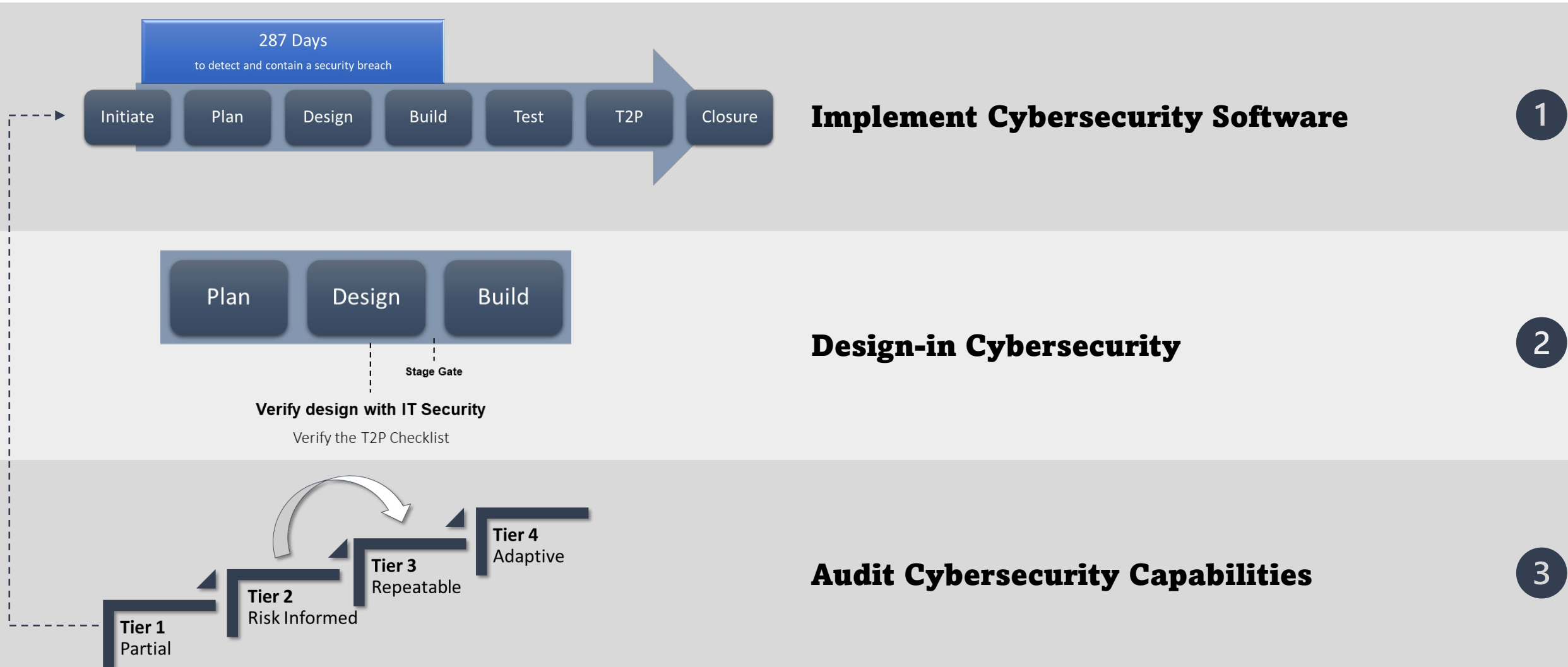


1. Greg Skulmoski, "Project Maturity and Competence Interface," *Cost Engineering*, Vol. 43, No. 6, June 2001,
2. Greg Skulmoski and John Schlichter, "Organisational Project Management Maturity: New Frontiers," *Project*, May 2000,
3. John Schlichter and Greg Skulmoski, "Organizational Project Management Maturity: New Frontiers," *Congress 2000, 15th IPMA World Congress on Project Management*, London, England, May 2000,
4. Ginger Levin and Greg Skulmoski, "Using a Project Management Maturity Assessment to Promote Project Management Improvements," *Managing Business by Projects*, Helsinki, Finland, September 16 - 17, 1999,
5. Francis Hartman and Greg Skulmoski, "Project Management Maturity," *Project Management*, Vol. 4, No. 1, 1998: 74-78.

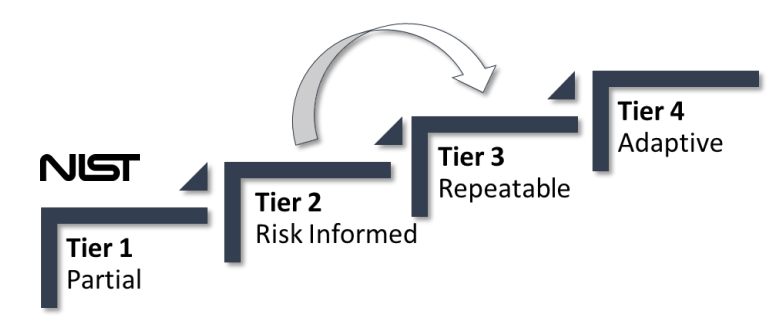
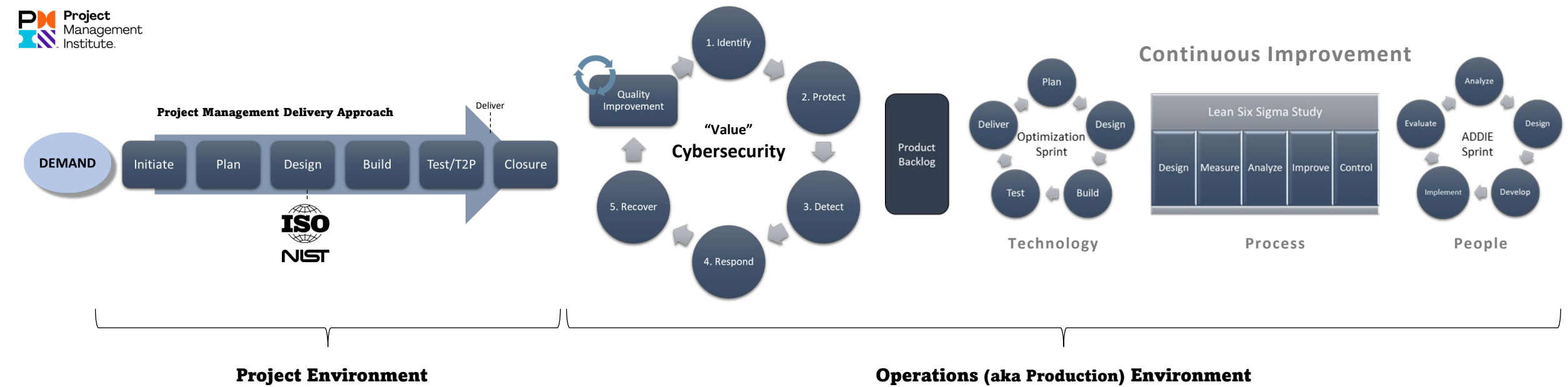


## Three Use Cases

# Cybersecurity Project Management

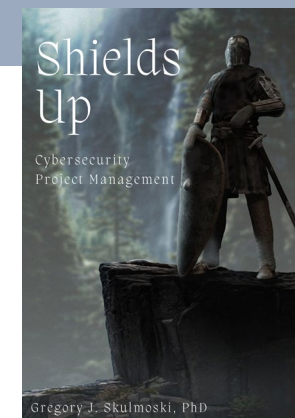


# Cybersecurity Project Management: Standards Alignment

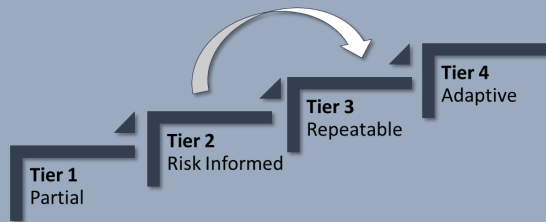
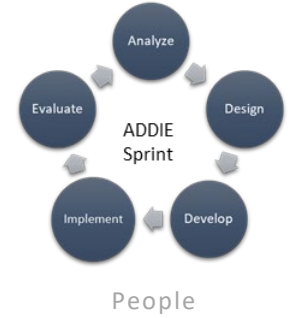
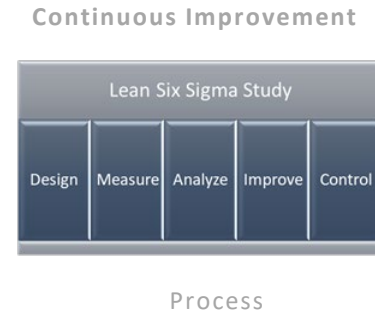
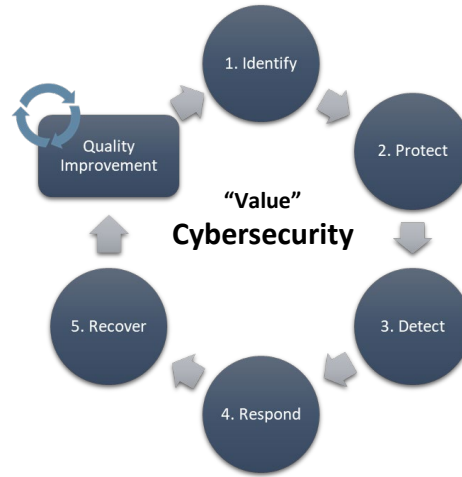
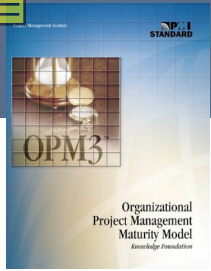


Logos for the following standards and organizations:

- NIST**
- PM Project Management Institute.**
- ITIL**
- ISO 9001 Quality Management**
- ISO 31000 Risk Management**
- ISO 27001 Information Security Management**



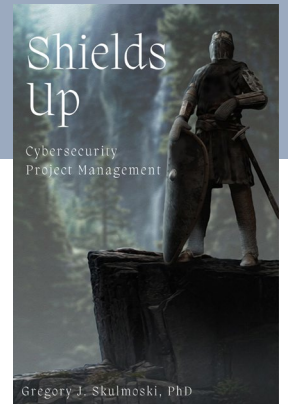
# Caution: Standards Compliance Focus

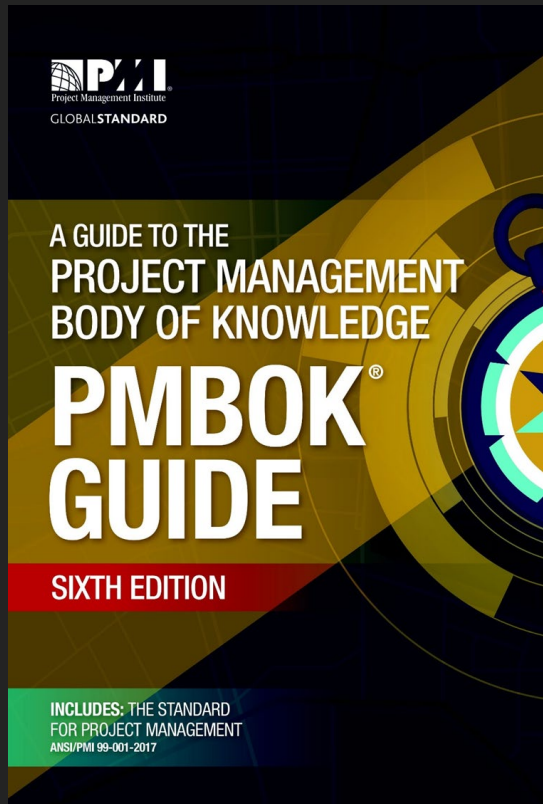


Compliance  $\neq$  Protection

Measure Cybersecurity Performance KPI's

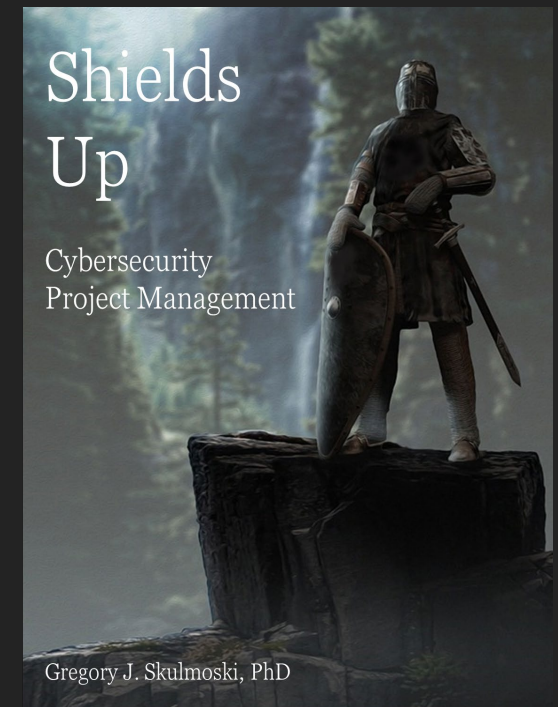
Protect, Detect, Respond, Recover



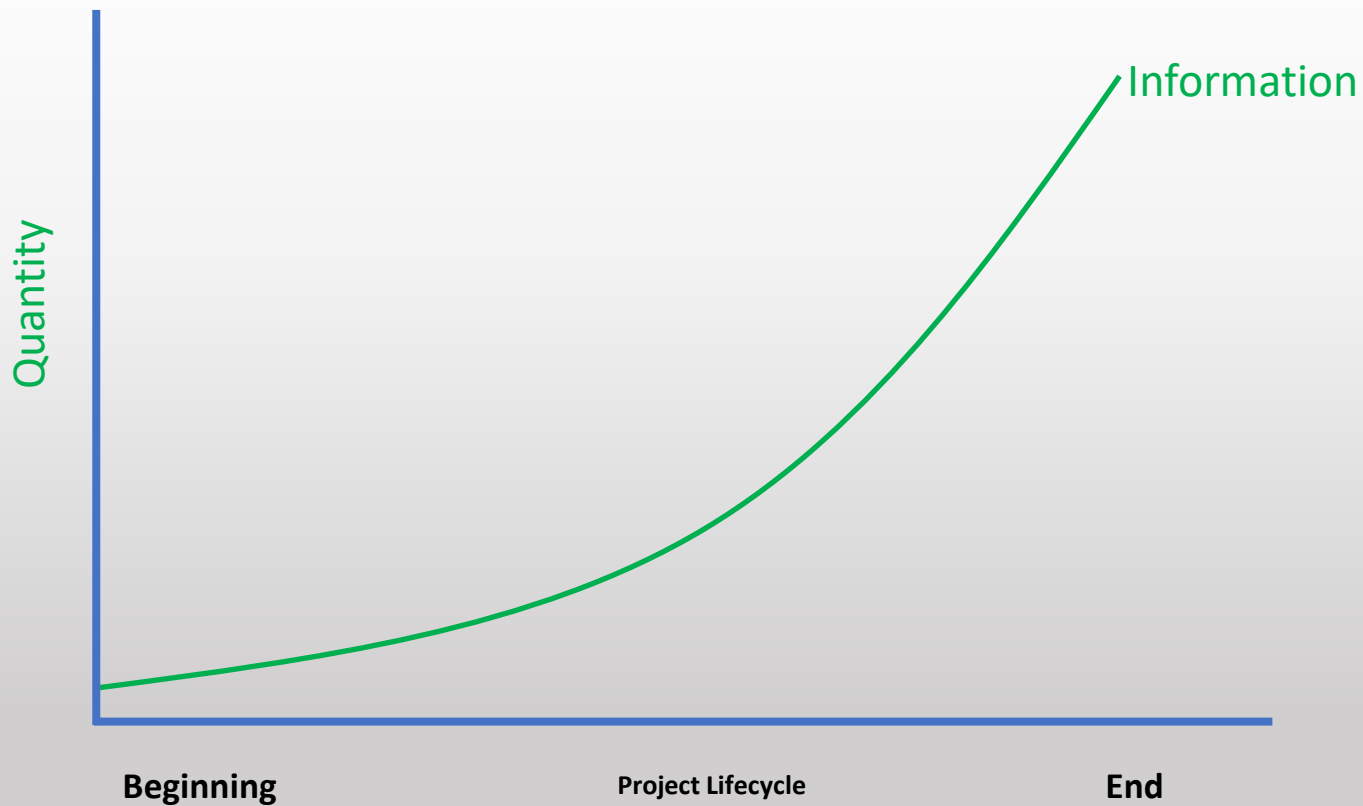


# Risk Management Technique

Not in the  
PMBOK® Guide

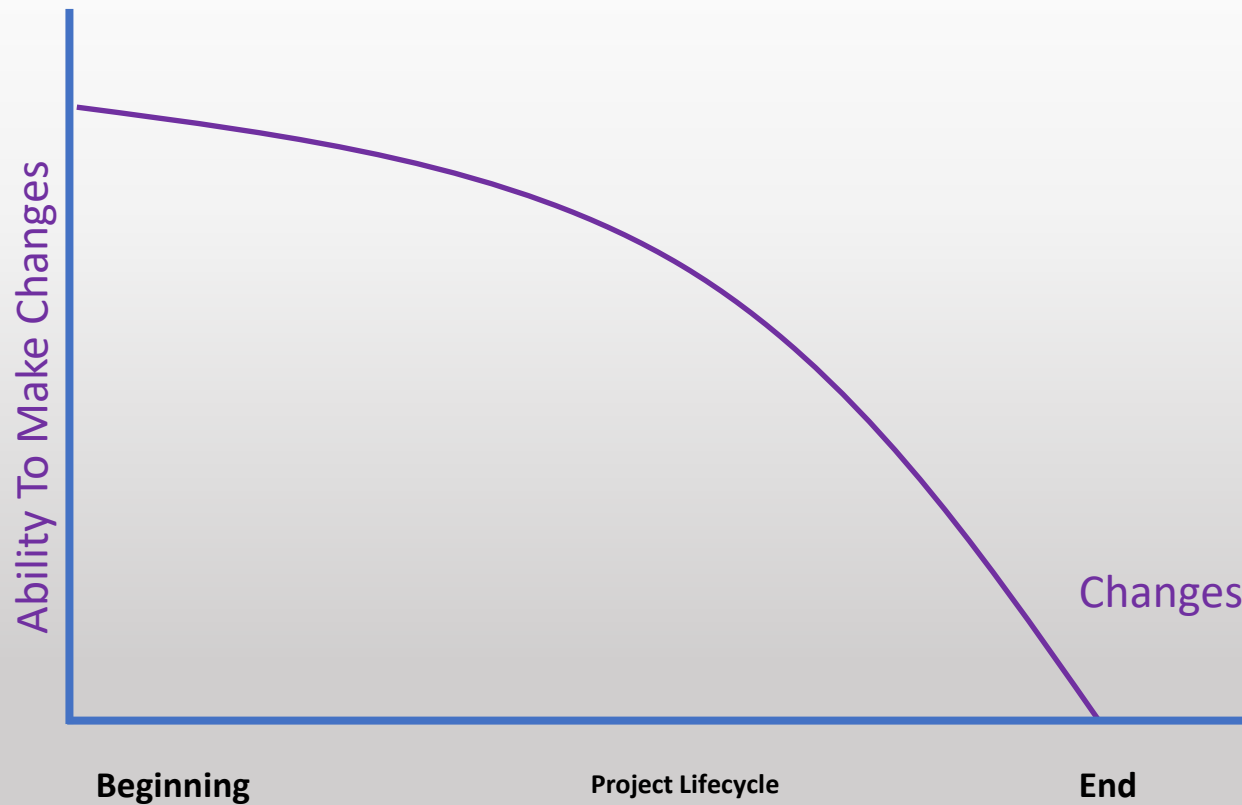


# Ability to Change Paradox



Lack of information at the beginning of the project

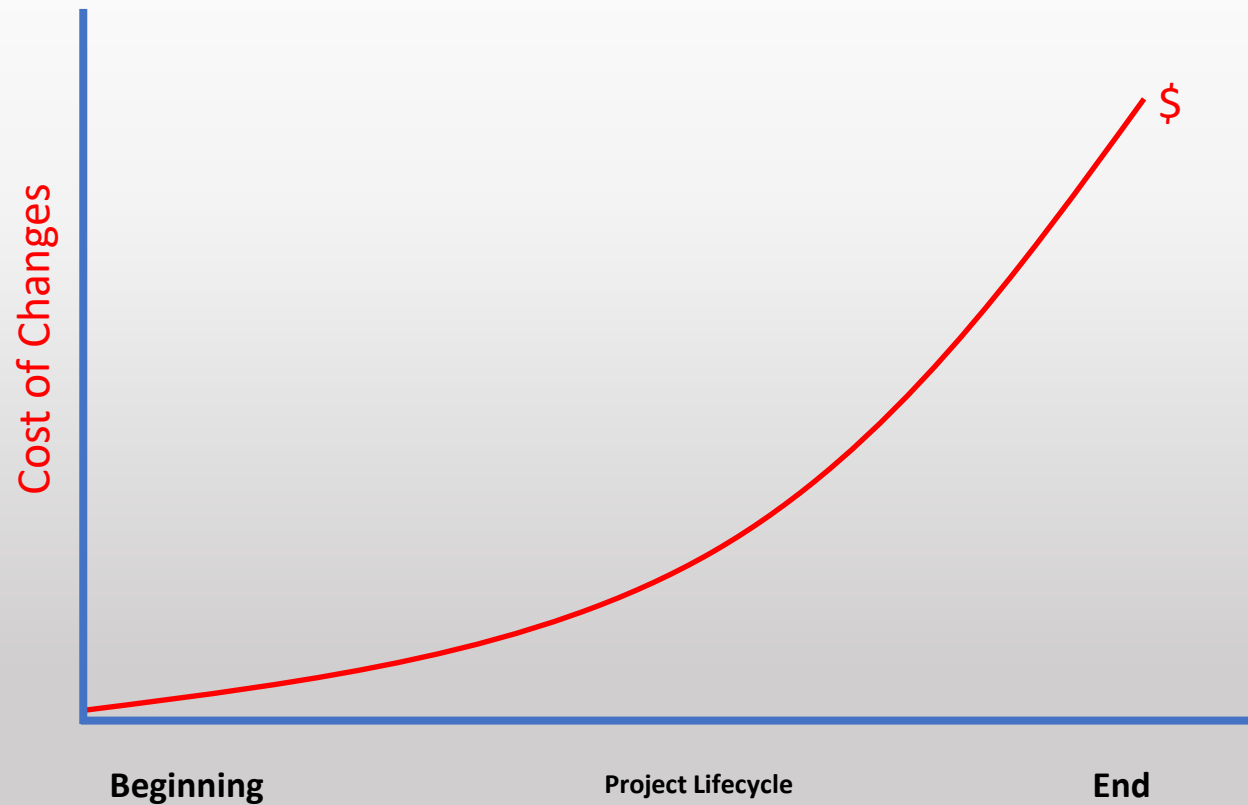
# Ability to Change Paradox



Changes are increasingly difficult to make

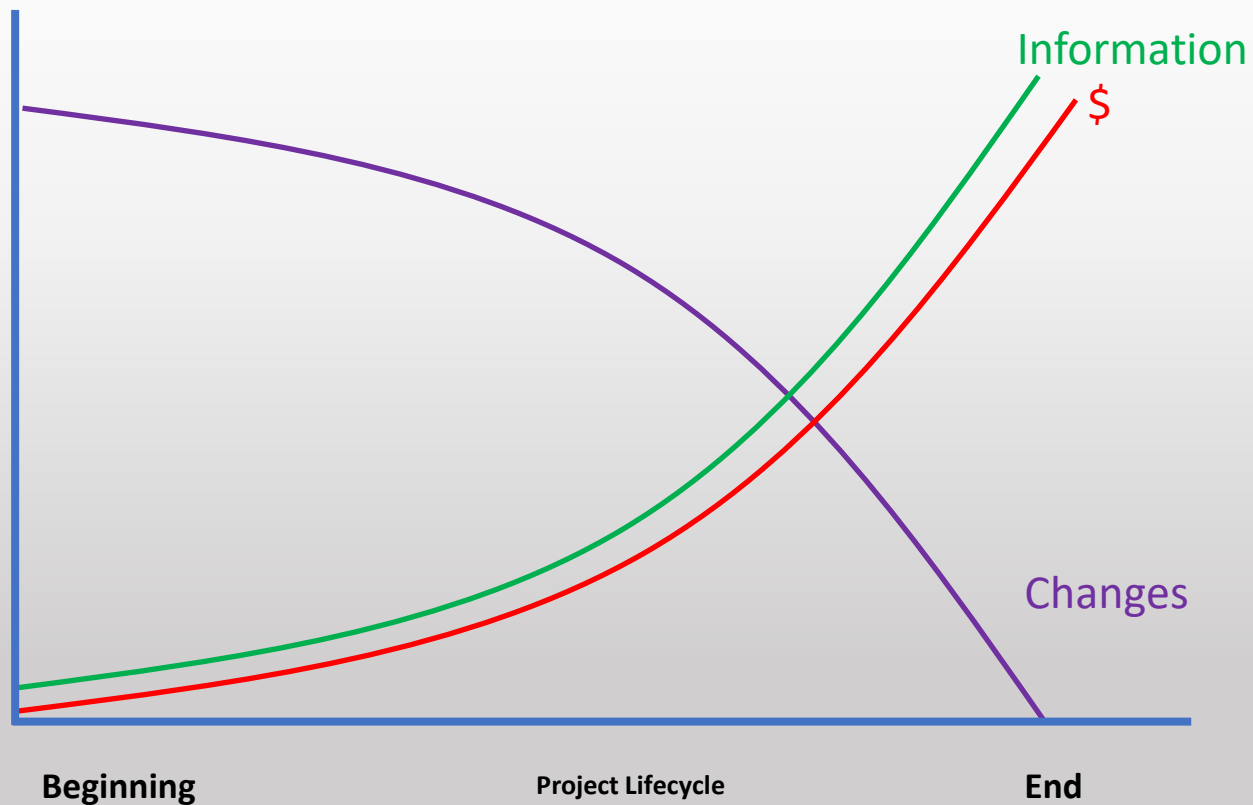


# Ability to Change Paradox



Changes are increasingly expensive to make

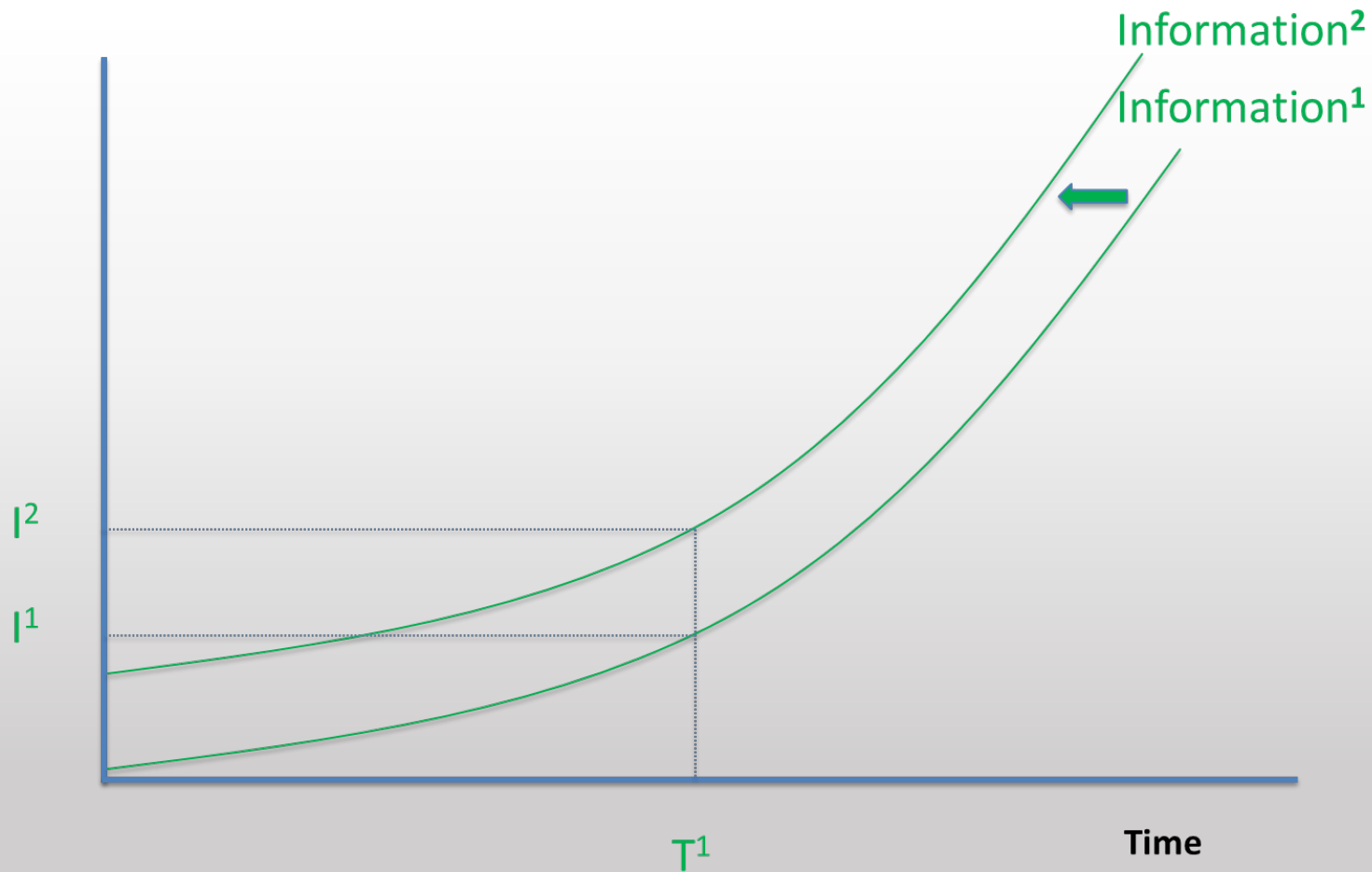
# Ability to Change Paradox



Paradox

When changes are the **easiest**, and least **costly**, we lack **information**

# Ability to Change Paradox



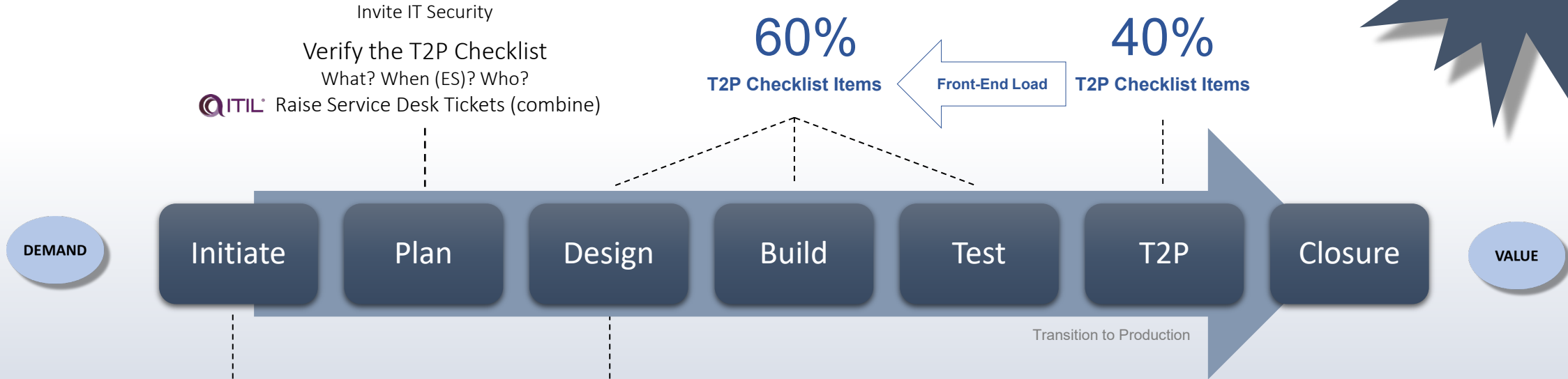
Solution

**Shift the  
Information  
Curve**

To learn more about  
our project sooner

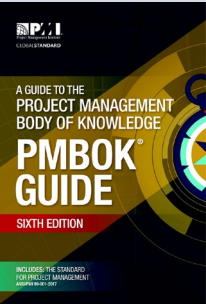
Risk  
Management!

# Shift the Information Curve: Front-End Load



12-hour days are easier at the start than at the end of a project

Bring work forward to create room in the future to address risks and leverage opportunities



absent

# Conclusion: Three Key Points

1

Cybersecurity is risk management



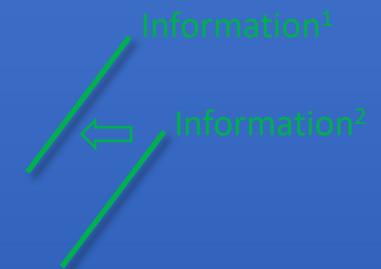
2

Project management underpins cybersecurity

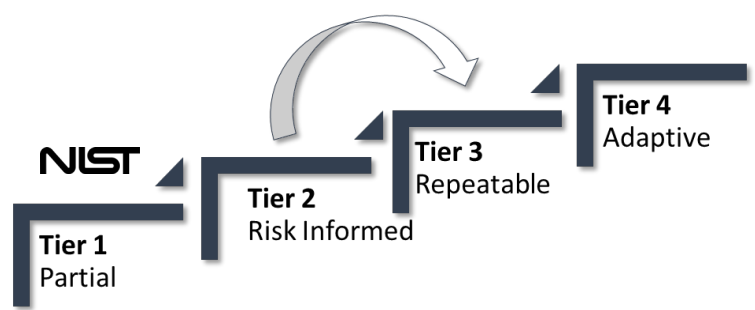
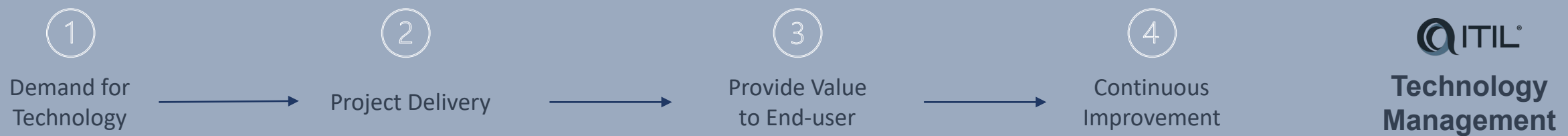
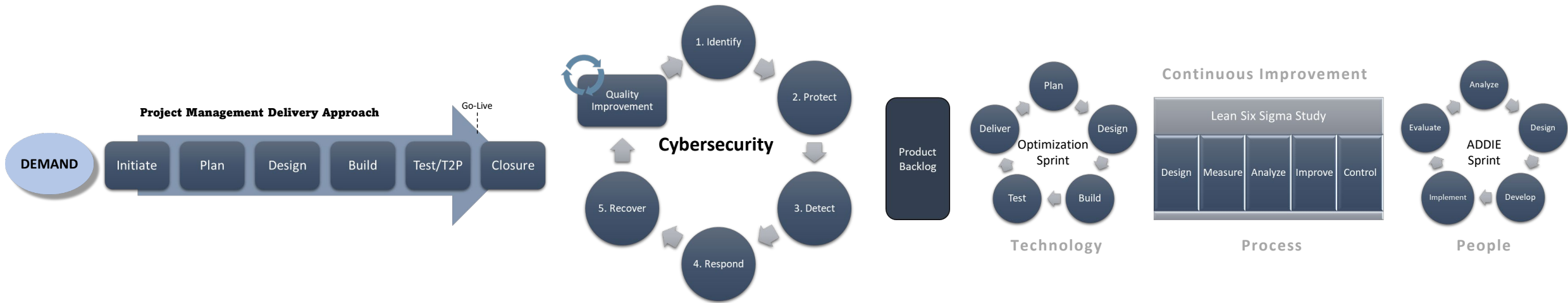


3

Front-end-load to shift the information curve



# Cybersecurity Project Management



**NIST**

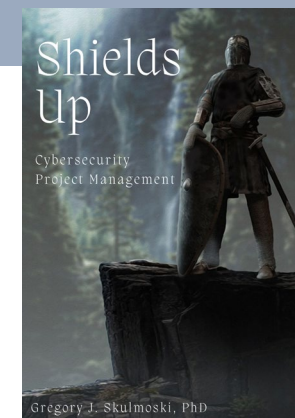
**PMI** Project Management Institute.

**ITIL**

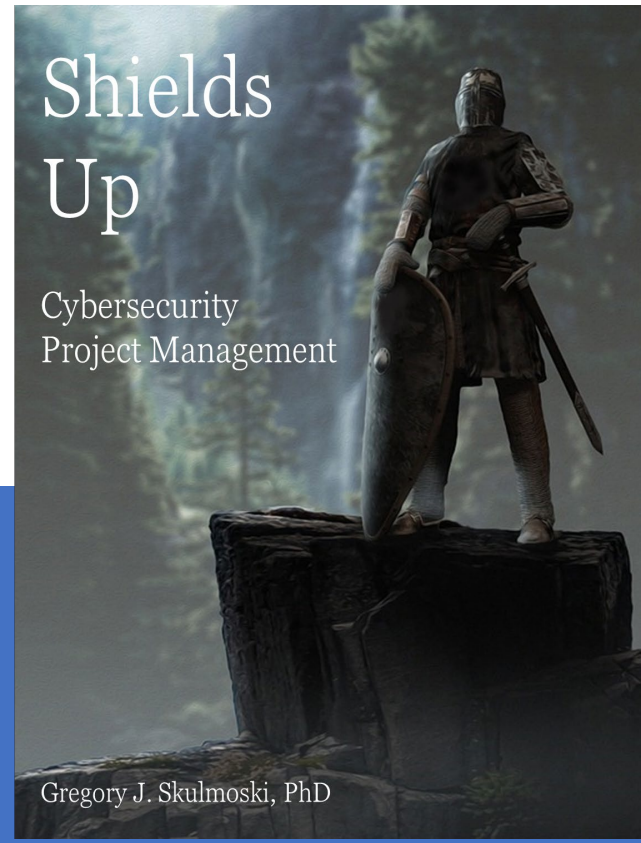
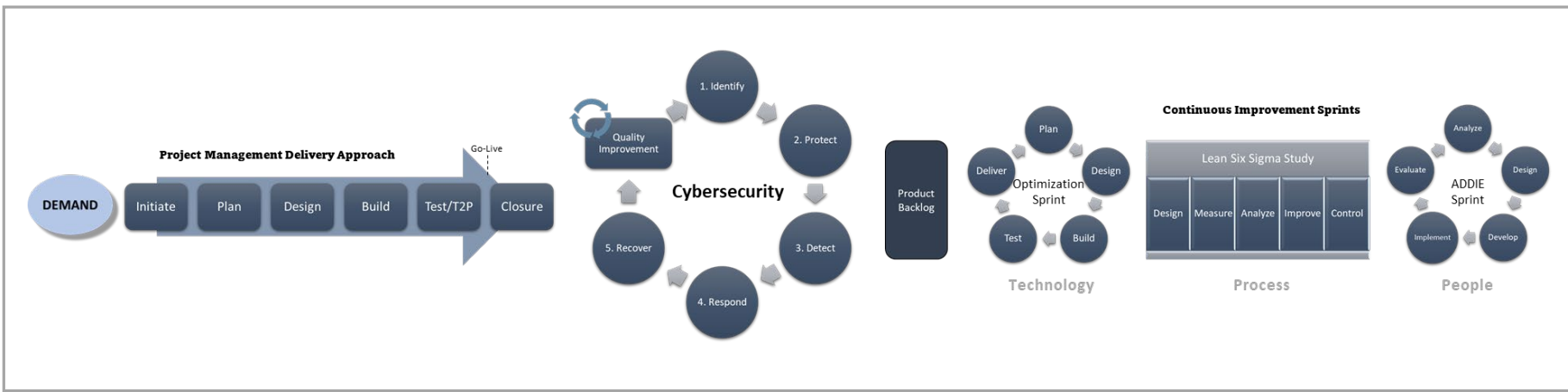
**ISO** ISO 9001 Quality Management

**ISO** ISO 31000 Risk Management

**ISO** ISO 27001 Information Security Management







\*\*\*\*\* Advance Praise \*\*\*\*\*

### “Must Read”

Jason Roos, Chief Information Officer  
King Abdullah University of Science and  
Technology, Saudi Arabia

### “Best I Have Seen In My Career”

Distinguished Professor Emeritus Timothy Kloppenborg PhD,  
Project Management  
Xavier University, United States

### “Unique Resource”

Professor Craig Langston PhD, Project Management  
Bond University, Australia

### “A Solid Guide”

Thiago Santos, Senior Technical Architect  
Mulesoft, Canada

### “Critical Tools”

Derek Molnar, PMP, Project Manager  
University of Colorado, United States

### “Perfect Alignment”

Irene Corpuz, PMP, ITIL, CISA, CEH, ISO 27001  
Lead Implementer & Auditor, Manager Projects  
Federal Higher Education, United Arab Emirates



United Nations Sustainable Development Goal #9: **Recognizable Contribution**

# Discussion



Greg Skulmoski PhD, MBA, BEd, CITP, FBCS  
Associate Professor, Project Innovation Management  
Faculty of Society and Design

