PRESENTED BY

BetterCloud
MONITOR

Creating a Security Blueprint

A Realistic Approach Using the CIS 20

Alijohn Ghassemlouei
Senior Information Security Consultant, *Bishop Fox*

WHAT ARE WE GOING TO TALK ABOUT?

COVERAGE

- What is the CIS 20?
- How does it affect me?
- Is it useful?
- What can I expect to get out of this?
- How do I use it?
- When are the donuts distributed?

WHO IS TALKING HERE?

ALIJOHN GHASSEMLOUEI

- Bachelors of Science in Network Security
- U.S. Department of Energy Contractor for 3 years
- Co authored “The Hacker's Guide to OS X: Exploiting OS X from the Root Up”
- U.S. Department of State Contractor for 1 year
- Sony PlayStation Worldwide Studios for 2 years
- Black Hat and DEF CON volunteer since 2008

STRUCTURE

UNDERSTANDING THE CRITICAL SECURITY CONTROLS

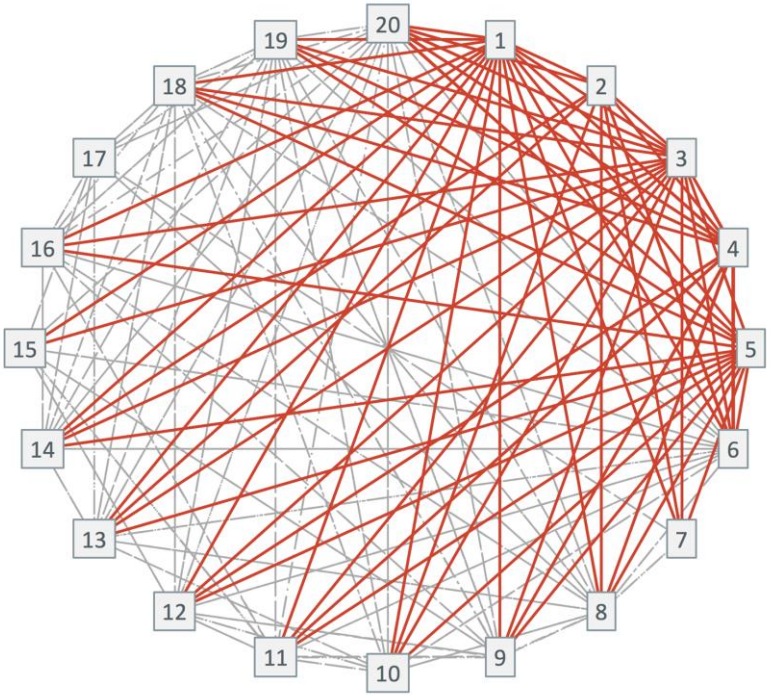
DEFINITION

WHAT IS THE CIS 20?

- Center for Internet Security (CIS) Critical Security Controls (CSC) version 6.1
- 20 high-level controls consisting of 149 sub-controls
- Specific and actionable ways to mitigate the risk of common security threats
- Informed by actual attacks and effective defenses
- Five tenants: offense informs defense, prioritization, metrics, continuous diagnosis/mitigation, and automation

RELATIONSHIPS & DEPENDENCIES

CIS 20 CRITICAL SECURITY CONTROLS



1	Inventory of Authorized and Unauthorized Devices
2	Inventory of Authorized and Unauthorized Software
3	Secure Configurations for Hardware and Software
4	Continuous Vulnerability Assessment and Remediation
5	Controlled Use of Administrative Privileges
6	Maintenance, Monitoring, and Analysis of Audit Logs
7	Email and Web Browser Protections
8	Malware Defenses
9	Limitation and Control of Network Ports, Protocols, and Services
10	Data Recovery Capability
11	Secure Configurations for Network Devices
12	Boundary Defense
13	Data Protection
14	Controlled Access Based on the Need to Know
15	Wireless Access Control
16	Account Monitoring and Control
17	Security Skills Assessment and Appropriate Training to Fill Gaps
18	Application Software Security
19	Incident Response and Management
20	Penetration Tests and Red Team Exercises

THE BENEFITS

CONSIDERATIONS

- Effective and specific set of technical measures to detect, prevent, and mitigate damage from the most common and damaging attacks.

- A well-understood, replicable, measurable, scalable, reliable, automatable, and continuous process.

- Comprehensive executive and technical reports with raw data, findings, recommendations, and insight into risk.

- Custom tailored methodology and templates to use for future self-assessments.

RELATIONSHIPS TO COMPLIANCE FRAMEWORKS

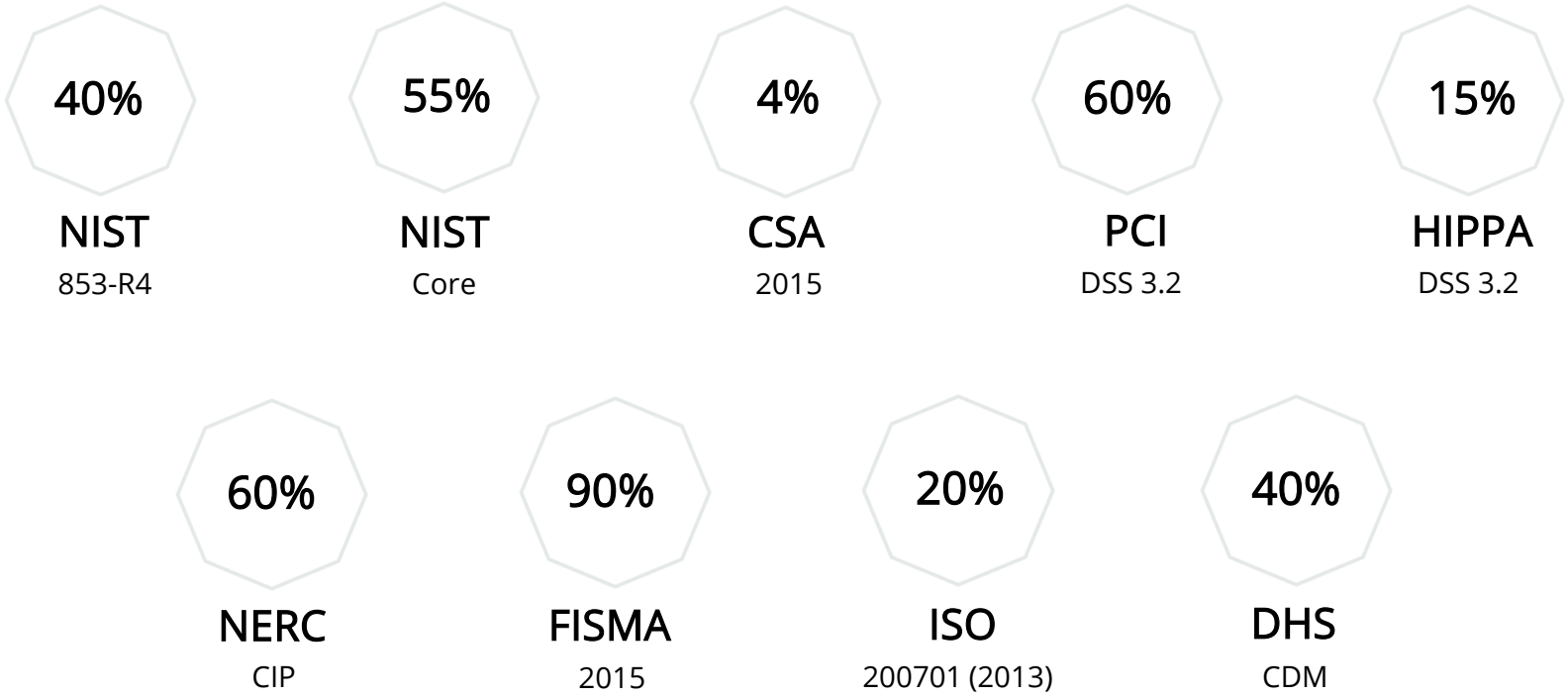
FRAMEWORK MAPPING

ID	Description	CSA	HIPPA	NIST 800-53	ISO 200701	PCI DSS 3.0	DHS CDM	NSA MNP	NERC CIP v5	NIST Core	FISMA 2015
1	Inventory of Authorized and Unauthorized Devices	3	2	7	3	1	2	6	2	3	2
2	Inventory of Authorized and Unauthorized Software	4	2	10	2	0	2	3	-	2	2
3	Secure Configurations for Hardware and Software	4	2	16	3	4	1	4	2	1	1
4	Continuous Vulnerability Assessment and Remediation	4	2	6	2	3	1	3	2	5	1
5	Controlled Use of Administrative Privileges	7	2	9	10	8	-	3	3	4	1
6	Maintenance, Monitoring, and Analysis of Audit Logs	2	2	17	5	7	1	1	1	7	0
7	Email and Web Browser Protections	4	2	16	3	4	1	4	2	1	1
8	Malware Defenses	4	4	6	3	4	-	5	1	3	1
9	Limitation and Control of Network Ports, Protocols, and Services	3	2	11	4	1	1	2	1	2	0
10	Data Recovery Capability	0	4	3	2	4	-	1	-	1	0
11	Secure Configurations for Network Devices	6	-	12	3	4	2	6	2	3	1
12	Boundary Defense	5	-	11	6	6	1	9	3	4	3
13	Data Protection	7	5	13	5	4	-	4	1	4	1
14	Controlled Access Based on the Need to Know	3	3	10	3	7	2	5	4	6	0
15	Wireless Access Control	4	-	10	3	2	-	5	1	-	0
16	Account Monitoring and Control	8	9	11	10	5	1	3	3	3	1
17	Security Skills Assessment and Appropriate Training to Fill Gaps	2	4	9	1	1	1	1	2	5	1
18	Application Software Security	7	-	11	6	4	1	1	-	1	0
19	Incident Response and Management	5	1	9	7	1	2	1	3	13	1
20	Penetration Tests and Red Team Exercises	-	-	8	3	1	-	1	-	-	0

Source - AuditScripts CIS 20 Master Mappings Tool (v6.0a) (2015)

INDIVIDUAL INSTANCES

UNIQUE MAPPING



STRATEGIC AND TACTICAL APPROACHES

COMPLIANCE vs REALITY

Compliance Frameworks

- Structures processes
- Establishes consistency
- Enforces accountability

CIS 20

- Actionable
- Broader topics
- Technical specifics

TARGET AUDIENCE

You? Me! No, You!

THE FOUR CHARACTERS

ENVIRONMENT

- What's the cloud?
- I don't trust clouds.
- ½ my things are in the cloud.
- Everything is in the *cloud*.

INDIVIDUAL INSTANCES

APPLICABILITY

- Where does my data live? How do I access it?
- How do I authenticate against everything?
- What happens when I get compromised?
- What happens if my internet connection drops?
- Can XYZ solution be customized to my needs?
- How much will all this cost?!
- Do we care about vendor assessments?
- Do I need a cloud security strategy?
- How am I going to handle my MSA/PSA with these cloud solutions?
- Why does my phone matter?
- What am I going to do without my proxy!
- How do I monitor anything!?
- What about wireless?
- Do I even care about awareness training?
- I should be completely fine with just Amazon services, right?

WILL THIS DRIVE CHANGE?

IMPACT

- How is this going to actually drive any change?
    - Magic.

ASSESSMENT METHODOLOGY

How does it all work?

HIGH-LEVEL ASSESSMENT APPROACH

THE RULE OF THREE

1. Identify the current state of technical controls implementation
   - Review existing documentation, including policies, processes, and procedures
   - Conduct on-site interviews with all stakeholders and IT support staff
2. Establish a baseline to measure security posture improvements
   - Leverage a tailored capability maturity model
   - Rate controls based off of evidence of implemented controls
3. Recommend next steps for security program development
   - High-level executive overview, findings, recommendations, risks, and roadmap
   - Conduct outbrief and technical report walkthroughs

HOW DEEP DO WE WANT TO GO?

GRANULARITY

- Discussions, meetings, and interviews
- Lightweight evidence collection
- Programmatic verification
- Technical verification

INTERNAL DELIVERABLES

OUTCOMES

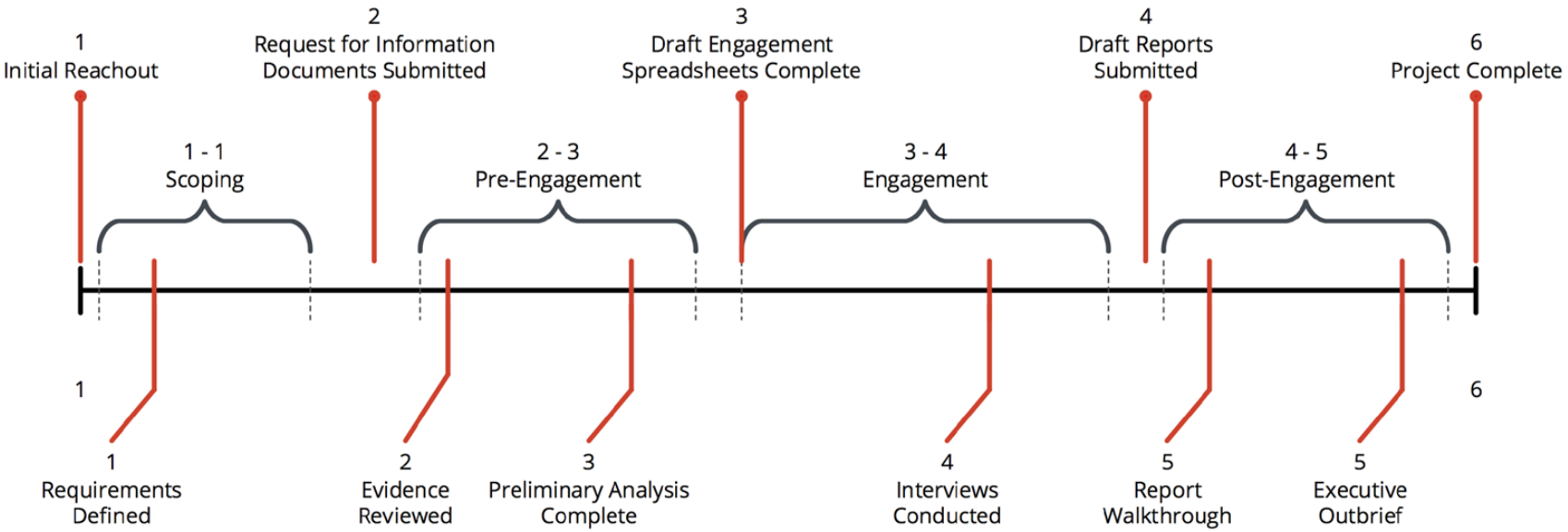
- Executive Report
- Executive Outbrief
- Tailored Technical Reports
- Strategic Roadmap
- Analysis on Actual Implementation
- Recommendations
- Identification of Preliminary Risk

THE ASSESSMENT LIFECYCLE

ASSESSMENT APPROACH

IDEAL ASSESSMENT IN PHASES

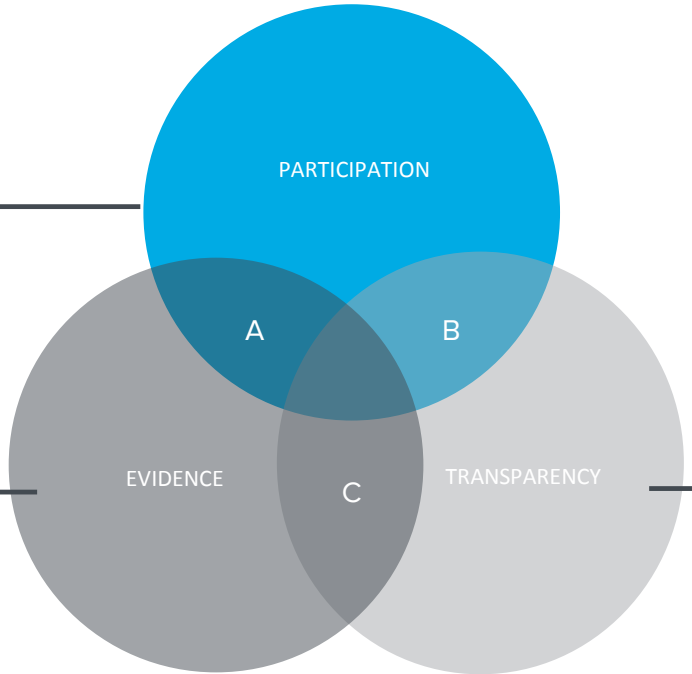
TIMELINE



BRIEF OVERVIEW

SUCCESS CRITERIA

Increased involvement leads to a faster and more comprehensive assessment



Comprehensive, factual, and relevant pieces of evidence provided

Non-adversarial atmosphere provides additional perspective into historical issues

INDIVIDUAL INSTANCES

COMMUNICATION

- Introduction of assessment team and processes
- POC identification begins, request for evidence sent over

- Re-communication of assessment needs
- Evidence collection status update

- Meetings scheduled, evidence collection communicated
- Stakeholder information collected

INDIVIDUAL INSTANCES

COMMUNICATION

- Who are *they*?
  - Is Amazon a person?
    - Do they like donuts?
  - The security POC for Heroku isn't responding..
    - Should send donuts.
- How do I communicate with them?
- Do they have backup contacts?
- Do they understand their roles?

LEVEL OF EFFORT

QUICK AND DIRTY?

- Where do I want to start?
- Is this a one time thing?
- Quick assessment?
- Full blown effort with rating tracking

LEVEL OF EFFORT

EVIDENCE

- What is evidence?
- Do you care?
- How do you collect it?
- What am I going to do with it?

LEVEL OF EFFORT

RATINGS

- How do I rate these things?
- What model or scale do I use?
- Can I make my own?
- What about weighting?
    - Aren’t all controls equal?
- Can I reprioritize things?

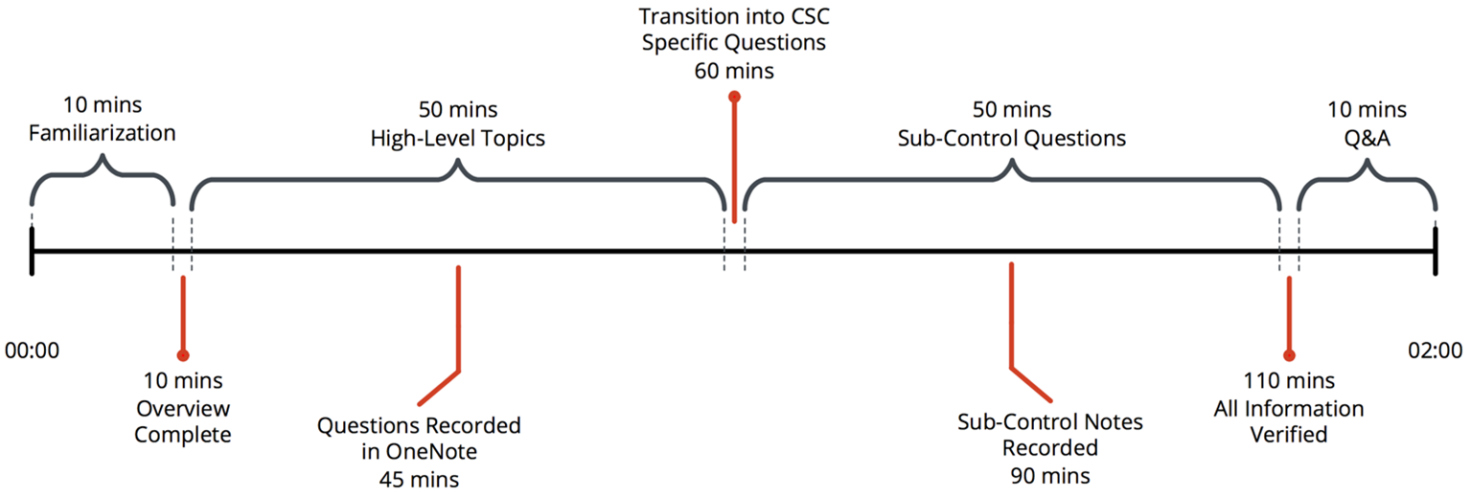
CMM MODEL

RATINGS

100	**Level 5 - Comprehensive** 100%	Processes have been refined to represent good practice, based on their measurable effects and comparison with other organizations. Technology is used to automate the workflow in an integrated way, providing tools to improve quality and effectiveness and making the enterprise quick to adapt.
80	**Level 4 - Managed & Measurable** 80-99%	It is possible to monitor and measure compliance with procedures and to take action where processes appear to be ineffective. Processes are constantly improved. Automation and tools are used in a limited or fragmented way.
60	**Level 3 - Defined** 60-79%	Procedures have been standardized, documented, and communicated through training. It is, however, left to the individual to follow these processes, and it is unlikely that deviations will be detected. The procedures themselves are not sophisticated, but are the formalization of existing practices.
40	**Level 2 - Repeatable** 40-59%	Different people undertaking the same task follow similar procedures. There is no formal training or communication of standard procedures, and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and, therefore, errors are likely.
20	**Level 1 - Initial / Ad Hoc** 20-39%	There is evidence that the organization recognizes that issues exist and need to be addressed. There are no standardized processes, but there may be ad hoc approaches that are applied on an individual or case-by-case basis. The overall approach to management is disorganized.
0	**Level 0 - Weak** 0-19%	Risk management processes are absent. The organization has not recognized that issues need to be addressed.

INDIVIDUAL INSTANCES

MEETINGS



CMM MODEL

RATINGS

100

Level 5 Optimized

100%

Processes have been refined to represent good practice, based on their measurable effects and comparison with other organizations.

Technology is used to automate the workflow in an integrated way, providing tools to improve quality and effectiveness and making the enterprise quick to adapt.

80

Level 4 Managed & Measurable

80-99%

It is possible to monitor and measure compliance with procedures and to take action where processes appear to be ineffective.

Processes are constantly improved. Automation and tools are used in a limited or fragmented way.

60

Level 3 Defined

60-79%

Procedures have been standardized, documented, and communicated through training.

It is, however, left to the individual to follow these processes, and it is unlikely that deviations will be detected.

The procedures themselves are not sophisticated, but are the formalization of existing practices.

40

Level 2 Repeatable

40-59%

Different people undertaking the same task follow similar procedures.

There is no formal training or communication of standard procedures, and responsibility is left to the individual.

There is a high degree of reliance on the knowledge of individuals and, therefore, errors are likely.

20

Level 1 Initial / Ad Hoc

20-39%

There is evidence that the organization recognizes that issues exist and need to be addressed.

There are no standardized processes, but there may be ad hoc approaches that are applied on an individual or case-by-case basis.

The overall approach to management is disorganized.

0

Level 0 Weak

0-19%

Risk management processes are absent.

The organization has not recognized that issues need to be addressed.

STRENGTHS, WEAKNESSES, AND FINDINGS

IDENTIFICATION

- How do I get out what I care about?

OUTPUT AND DELIVERABLES

WHAT DID I GET OUT OF ALL THIS?

- What are my assessment results going to do?
- Seriously. What?

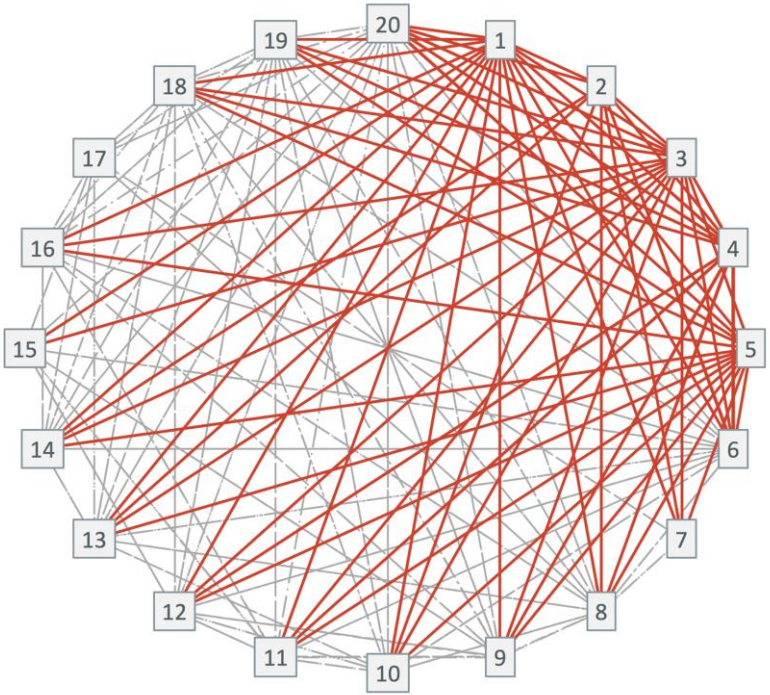
INDIVIDUAL INSTANCES

WHAT ABOUT THE NEXT STEPS?

- Develop cloud security strategy
- Queue up necessary resources
- Bring whiteboards and donuts.

RELATIONSHIPS & DEPENDENCIES

CIS 20 CRITICAL SECURITY CONTROLS



1	Inventory of Authorized and Unauthorized Devices
2	Inventory of Authorized and Unauthorized Software
3	Secure Configurations for Hardware and Software
4	Continuous Vulnerability Assessment and Remediation
5	Controlled Use of Administrative Privileges
6	Maintenance, Monitoring, and Analysis of Audit Logs
7	Email and Web Browser Protections
8	Malware Defenses
9	Limitation and Control of Network Ports, Protocols, and Services
10	Data Recovery Capability
11	Secure Configurations for Network Devices
12	Boundary Defense
13	Data Protection
14	Controlled Access Based on the Need to Know
15	Wireless Access Control
16	Account Monitoring and Control
17	Security Skills Assessment and Appropriate Training to Fill Gaps
18	Application Software Security
19	Incident Response and Management
20	Penetration Tests and Red Team Exercises

REACH OUT

CONTACT INFORMATION

Alijohn Ghassemlouei
Senior Information Security Consultant

Email aghassemlouei@bishopfox.com
Skype aghassemlouei
Twitter @X72

BISHOP FOX®

Q&A

JOIN THE CONVERSATION! bettercloud.com/slack-community

CLOUD IT LIVE

PRESENTED BY

BetterCloud MONITOR

COMING UP NEXT:

How You Can Benefit by Implementing Android for Work @ 4:45pm ET

SUPPLEMENTARY

ADDITIONAL PRESENTATION RESOURCES

DIRECT VIDEO DOWNLOAD

VIEW or **DOWNLOAD**

CREATING A SECURITY BLUEPRINT - A REALISTIC APPROACH USING THE CIS 20

ABSTRACT

What's more important – security or compliance? Wouldn't it be great to kill two birds with one stone? Good news – you can! There is a roadmap specifically developed to help you create a comprehensive and immediately actionable guide for a more secure organization – it's called the CIS 20.

The CIS 20 is a set of security controls designed to give priority and focus to your journey towards effective and transparent security. Unfortunately, standards and frameworks are often misinterpreted, leading to technologies and safeguards that only address the minimum requirements. In this talk, we'll discuss each of the recommended actions and its real world effectiveness to help you create a security blueprint for your organization, even if it's entirely in the cloud.

With a thorough understanding of the CIS 20, you'll know your current security posture and what is needed to harden your defenses. Let this talk be your guide as you navigate the treacherous waters of compliance and security. Understanding your organization's security posture can be a daunting task, but it can be done. Step one, bring donuts. Step two, stay calm. Step three, sit in and learn how.

Attributions (Images in Slides)

Suit image