NH PTAC
CMMC Maturity Level 3

An overview of the CMMC, how we got here, and how to help organizations move forward at Maturity Level 3.

- Joe Kurlanski, CISSP®, HCISPP®
- jkurlanski@monarchisc.com
- 207-808-0472 (o)
- 207-232-2511 (c)

MONARCH ISC
INFORMATION SECURITY CONSULTING

Today's Agenda

- Prologue (How we got here)
- NIST SP 800-171
- CMMC Today
- Deep Process Dive
- "5 and 5" – Easy Wins and Long-Term Priorities
- Where to Start & How We Can Help

MONARCH ISC
INFORMATION SECURITY CONSULTING

Prologue

- Health Insurance Portability and Accountability Act (HIPAA Security Rules - 1996)
  - Very generalized.
  - Applied to all covered entities with protected health information (PHI) including insurers and hospitals, to sole-practitioners.
  - No penalties + no audits = no compliance.
  - HITECH Act (2009) enforces “Business Associate” requirements and introduces rewards for compliance.
- Gramm Leach Bliley Act (GLBA-1999)
  - Generalized, but directed the banking oversight organizations to create specific rules for enforcement, which they did.
  - Failed Audit could result in raised interest rates to borrow or in suspension of a bank’s charter to operate.
  - Penalty + Annual Audits = Fully Compliant and Mature Cyber programs.

MONARCH ISC
INFORMATION SECURITY CONSULTING

Prologue

- Payment Card Industry Data Security Standard (PCI-DSS 2004)
  - Very Specific.
  - Combination of Self-Assessment and Auditors.
  - Non-compliance = marginally higher fees.
  - Some retailers decide its easier to pay the fees.
  - Introduced the idea of data segregation and removing card holder data from the environment.
- NIST SP 800-171 (2015)
  - Specific controls for systems with **Controlled Unclassified Information (CUI)**
  - Self-Assessments only.
  - No penalties + limited audits = limited compliance.
  - Nota Bene: The DoD believes a contractors are compliant!

MONARCH ISC
INFORMATION SECURITY CONSULTING

Prologue: Lessons Learned

- Audits = Compliance
- If you don’t need the data, get rid of it (securely).
- If you do need it, isolate the systems to reduce the scope of the audit and your costs.
- DOCUMENT EVERYTHING.
- Don’t view compliance as an obstacle to doing business, because….
- …successful cybersecurity programs will enhance business operations AND sales.

MONARCH ISC
INFORMATION SECURITY CONSULTING

Prologue: More Lessons Learned

- Passing the audit is not the end of the journey
  - You are developing a new SOP.
  - Effective Cyber programs become institutional.
  - “Keep a clean kitchen, and never fear a health inspection.”
- This is not an IT problem to solve (or MSP).
  - Separation of duties = “doers” cannot effectively assess.
  - Documentation is not the strength of the IT professional.
  - Contract/Sub-Contract Management is not IT.
  - Governance/Legal is not IT.
  - Audit and Oversight development is not IT.

MONARCH ISC
INFORMATION SECURITY CONSULTING

NIST SP 800-171
(is dead, long live
NIST SP 800-171)

- Remember: it is specific to CUI.
- CMMC Maturity Level 3 includes the 110 controls.
- NO dates attached to this!
- The DoD thinks you are compliant since October 2017 if you have CUI and a signed contract (DFARS)
- Includes requirement to have a System Security Plan (SSP).

MONARCH ISC
INFORMATION SECURITY CONSULTING

Q4 2020
What Happened?

- DoD announces Scoring and Assessment strategy.
- Scores must be uploaded by contractors into Supplier Performance Risk System, along with POA&M and SSP.
- Primes blast letters pushing Sub compliance and requirement to submit scores.
- PUSH BACK IF NO CUI !!

https://www.acq.osd.mil/dpap/pdi/cyber/guidance_for_assessing_compliance_and_enhancing_protections.html

MONARCH ISC
INFORMATION SECURITY CONSULTING

SP 800-171 Assessment & Scoring Methodology

- Scoring: Start with a score of 110 and subtract 1,3, or 5 points for non-compliance.
- Basic: Submit self-assessment score + SSP + POA&M
- Medium: Same as Basic, and DoD will schedule a review of your SSP and POA&M and may ask for further evidence of control compliance.
- High: Same as Basic, and DoD will conduct onsite or remote audit of SSP and validate compliance with all controls.

https://www.acq.osd.mil/dpap/pdi/cyber/docs/NIST%20SP%20800-171%20Assessment%20Methodology%20Version%201.2.1%20%206.24.2020.pdf

MONARCH ISC
INFORMATION SECURITY CONSULTING

State of CMMC

- First 100 assessors are out the door.
- No one has a Cybersecurity Model Maturity Certification.
- The implementation is STILL provisional. This will change in 2021.
- CMMC-AB is preparing for ML 1 & 3.

MONARCH ISC
INFORMATION SECURITY CONSULTING

State of CMMC (cont.)

- DoD contractors must have active certification in SPRS when contract has been granted.
- CMMC is not required to bid on a contract, but there is ***no*** grace period afterwards.
- Assessment Guides released.
- Contracts rollout through 2025

MONARCH ISC
INFORMATION SECURITY CONSULTING

Projected rollout as of 2/2021

OUSD(A&S) is working with Services and Agencies to identify candidate programs for CMMC implementation during FY21-FY25 phased roll-out

Total Number of New Prime Contracts Awarded Each Year with CMMC Requirement				
FY21	FY22	FY23	FY24	FY25
15	75	250	479	479

	Total Number of Prime Contractors and Sub-Contractors with CMMC Requirement				
	FY21	FY22	FY23	FY24	FY25
Level 1	899	4,490	14,981	28,714	28,709
Level 2	149	749	2,497	4,786	4,785
Level 3	452	2,245	7,490	14,357	14,355
Level 4	0	8	16	24	28
Level 5	0	8	16	24	28
Total	1,500	7,500	25,000	47,905	47,905

All new DoD contracts will contain the CMMC requirement starting in FY26

MONARCH ISC
INFORMATION SECURITY CONSULTING

CMMC Breakdown Don't Forget Processes

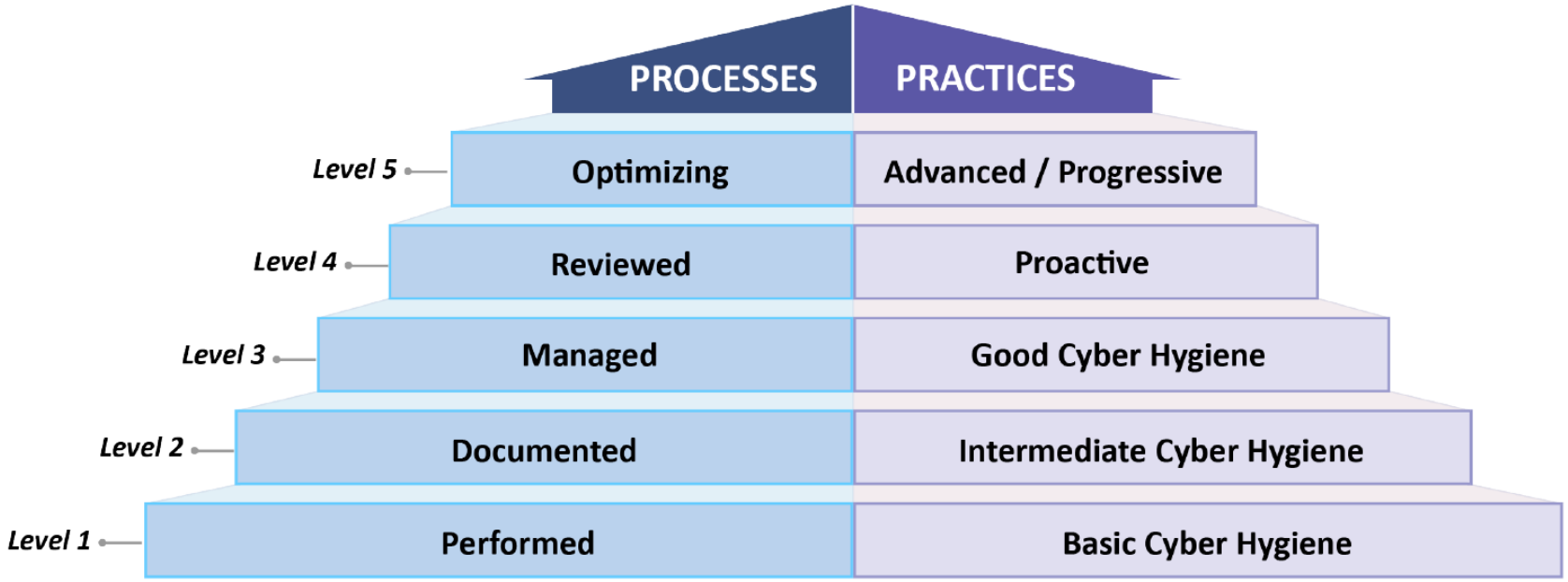


Figure 2. CMMC Levels and Descriptions

MONARCH ISC
INFORMATION SECURITY CONSULTING

Maturity in Two Dimensions:
Practices

- Level 1: Basic Cyber Hygiene (17 Practices)
  - Just getting started
  - Limited set of controls
  - Ad-hoc, not consistent
- Level 2: Intermediate Cyber Hygiene (72)
  - Bridge to complete 800-171 control set
  - Other control frameworks are represented

MONARCH ISC
INFORMATION SECURITY CONSULTING

Maturity in Two Dimensions: Practices

- **Level 3: Good Cyber Hygiene (130)**
  - Protection of CUI
  - Full NIST 800-171 (plus 20 more)
- Level 4: Proactive (156)
  - Advanced Persistent Threats (APTs)
  - Enhanced subset from 800-171B
  - Detection & Response capabilities
- Level 5: Advanced/Proactive (171)
  - Increased sophistication
  - Sustainable through environmental changes

MONARCH ISC
INFORMATION SECURITY CONSULTING

Maturity in Two Dimensions:
Processes

- Level 1: Performed
  - Requires that you are doing it.
  - Process maturity not assessed at this level
- Level 2: Documented
  - Established & documented procedures and polices
  - Repeatable as documented
  - Beginnings of “Institutional Memory™”

MONARCH ISC
INFORMATION SECURITY CONSULTING

Maturity in Two Dimensions:
Processes

- Level 3: Managed
  - Documented security plan for how practices are performed, resourced.
  - Who does it? How? What tools?
  - What's the budget for this practice?
- Level 4: Reviewed
  - Measured for effectiveness
  - Correct if not operating as intended
  - Report performance / status "up"
- Level 5: Optimizing
  - Standardized in all organizational units and locations
  - Consistency = resilience (and protection of CUI)

MONARCH ISC
INFORMATION SECURITY CONSULTING

Deep Dive
Process Maturity
SI: System and Information Integrity

- Level 1 Practices
  - SI.1.210 – Identify, report, and correct information system flaws in a timely manner.
  - **SI.1.211 – Provide protection from malicious code at appropriate locations within the organizational information systems**
  - SI.1.212 – Update malicious code protection mechanisms when new releases are available
  - SI-1. 213 – Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

MONARCH ISC
INFORMATION SECURITY CONSULTING

Deeper Dive
Process Maturity
SI: System and Information Integrity – SI.1.211

Level 1 – Do it!

- In other words – install anti-virus!
- Assessment guide: “Are system components (e.g., workstations, servers, email gateways, mobile devices) where malicious code protection must be provided identified and documented?”
  - Inventory
  - Centrally managed

MONARCH ISC
INFORMATION SECURITY CONSULTING

Deeper Dive
Process Maturity
SI: System and Information Integrity – SI.1.211

Level 2: Do we have a policy?

- Policy is high-level language.
  - Company installs anti-malware software on all workstations.
  - Company maintains anti-malware protection on email gateways.
  - Anti-malware is centrally managed.
  - Anti-malware software is configured to prevent end users from tampering.
  - Anti-malware software will scan workstations daily.
  - Anti-malware is configured to check for updates automatically, but at least once every 12 hours.
  - Anti-malware status is checked daily by IT.
  - Anti-malware is configured to alert staff when malicious software is detected, updates fail, and/or if software is tampered with.
- Pro Tip: Make it easy on the auditor.

MONARCH ISC
INFORMATION SECURITY CONSULTING

Deeper Dive
Process Maturity
SI: System and Information Integrity – SI.1.211

Level 2: Do we have a procedure?

- Procedure – detailed enough for a trained individual to follow.
    1) Antimalware monitoring website is: https://AVMONITOR.COM
        1) Login with AD Credentials.
        2) User must be in AV MONITOR group.
        3) Check Reports -> Alerts daily.
        4) Check AV Status -> Workstations daily.
    2) AV workstation and Server setup:
        1) Disable user tampering
        2) Check AV at least twice a day
        3) Quick scan once every 12 hours
        4) Full scan once a week
    3) AV Alerting is setup to email all correct staff
        1) Login with AD Credentials.
        2) User must be in AV MONITOR group
        3) Realtine Alerts -> Message notifications. Includes IT Admins, Security, Help Desk.

MONARCH ISC
INFORMATION SECURITY CONSULTING

Deeper Dive
Process Maturity
SI: System and Information Integrity – SI.1.211

Level 3: How are We Doing It?

- Document how you are performing the practice.
- System Security Plan:
  - Sophos Antivirus is deployed to all workstations and servers.
  - Sophos Central management tool is checked daily by Help Desk Support II role and logged.
  - An annual budget of $X,000 is provided for licensing.

MONARCH ISC
INFORMATION SECURITY CONSULTING

Deeper Dive
Process Maturity
SI: System and Information Integrity – SI.1.211

Level 4: Is what we are doing working, and whom should we tell?

- Measuring effectiveness
  - Use malware tests to ensure detection and reporting on a regular basis.
- Report on metrics
  - Daily reporting of % Compliant with updates and scans.
  - Report to senior/executive leadership.
  - Regular scheduled reporting is recommended.

MONARCH ISC
INFORMATION SECURITY CONSULTING

Deeper Dive
Process Maturity
SI: System and Information Integrity – SI.1.211

Level 5: Are we doing it everywhere?

- Have we installed anti-malware on all workstations, or just those with CUI?
- Across all departments and locations.

MONARCH ISC
INFORMATION SECURITY CONSULTING

CMMC 5 & 5

5 Easy Wins

- The practices you can do without breaking the back or the bank

5 Long-term Plans

- The practices that are critical but will take long term planning and/or considerable resources.

MONARCH ISC
INFORMATION SECURITY CONSULTING

CMMC 5 & 5

5 Easy Wins

The practices you can do without breaking the back or the bank

MONARCH ISC
INFORMATION SECURITY CONSULTING

Beyond the Framework:
5 Easy Wins

One

- **AC.2.008** Use non-privileged accounts or roles when accessing non-security functions.
  - Do not use Administrator-level accounts to do daily business activities
  - Create a standard user account for each Admin
  - Only use privilege when privilege is required for the task.

MONARCH ISC
INFORMATION SECURITY CONSULTING

Beyond the Framework:
5 Easy Wins

Two

- **AT.2.056** Ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.
  - Annual Security and Awareness Training
  - Hire a third-party
  - Do it over video conference
  - Relatively inexpensive

MONARCH ISC
INFORMATION SECURITY CONSULTING

Beyond the Framework:
5 Easy Wins

Three

- **AU.2.041** Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.
  - Active Directory - Turn on logging
  - Directory Audit Logs
  - Firewall
  - Any system or device that can log, should log.

MONARCH ISC
INFORMATION SECURITY CONSULTING

Beyond the Framework:
5 Easy Wins

Four

- **SA.3.169** Receive and respond to cyber threat intelligence from information sharing forums and sources and communicate to stakeholders.
  - Vendor feeds specific to your environment
  - Government feeds
    - US-CERT
    - DHS
    - FTC
  - Industry feeds
    - Krebs on security
    - Bleeping Computer
    - SANS
  - ISACs – Information Sharing & Analysis Centers
    - https://www.nationalisacs.org/
    - National Defense ISAC: https://ndisac.org/
    - Maritime ISAC: https://maritimesecurity.org

MONARCH ISC
INFORMATION SECURITY CONSULTING

Beyond the Framework:
5 Easy Wins

Five

- **PE.1.133** Maintain audit logs of physical access.
  - Require visitors to sign a log
  - Require all personnel going into data center / server rooms sign a log
  - Keep the logs for at least one year

MONARCH ISC
INFORMATION SECURITY CONSULTING

Beyond the Framework

5 Long-Term Plans

Practices which will demand significant people, dollars, and/or time to implement.

MONARCH ISC
INFORMATION SECURITY CONSULTING

Beyond the Framework:
5 Long-Term Plans

One

- **AC.1.003 Verify and control/limit connections to and use of external information systems.**
  - This could be personally owned devices, contractors their own devices, or cloud services.
  - If segmenting your systems, its any system without access to Federal Contract Information (Level 1) or CUI (Level 3)
  - Start with a policy but determine if you will need Network Access Control (NAC), Mobile Device Management for personally owned devices, and/or training.
  - **CUI in the cloud = FedRAMP High requirements!**

MONARCH ISC
INFORMATION SECURITY CONSULTING

Beyond the Framework:
5 Long-Term Plans

Two

- **AU.2.044** Review audit logs.
  - Security Event and Information Management (SEIM)
    - Manage on-premises
    - Third-party managed service
  - Learning what is “normal” activity.

MONARCH ISC
INFORMATION SECURITY CONSULTING

Beyond the Framework:
5 Long-Term Plans

Three

- **IR.2.092** Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recover, and user response activities..
  - NIST 800-61r2
  - Create an Incident Response Team
  - Document preparation for being capable
  - Create a clear channel to report incidents
  - Document procedures for specific incident types

MONARCH ISC
INFORMATION SECURITY CONSULTING

Beyond the Framework:
5 Long-Term Plans

Four

- **FIPS MODE – Turn on when protecting CUI.**
- Using FIPS approved algorithms is not enough, the module must be validated.
  - AC.3.012 Wireless Access
  - AC.3.014 Remote Access
  - AC.3.022 Mobile Devices
  - MP.3.125 Digital Media
  - RE.2.138 Backups
  - SC.3.185 Data in Transmission
  - SC.3.191 Data at Rest
  - SC.3.177 Anywhere else we forgot to mention.

MONARCH ISC
INFORMATION SECURITY CONSULTING

Beyond the Framework:
5 Long-Term Plans

Five

- **IA.3.083** Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.
  - Turn-on MFA at MS 365, G Suite
  - Turn-on MFA on VPNs
  - Turn-on MFA for all network access for all users.
  - Turn-on MFA for all Administrator authentication

MONARCH ISC
INFORMATION SECURITY CONSULTING

Where Do We Start?

Find out where you are:

- Complete a compliance gap assessment.
- Be realistic about your implementation, documentation, and ability to produce examples of both during an audit.
- Create a plan of action and milestones (POA&M) – a road-map of actions to close gaps and achieve target CMMC maturity level, and more importantly, secure operations.

MONARCH ISC
INFORMATION SECURITY CONSULTING

Where Do We Start?

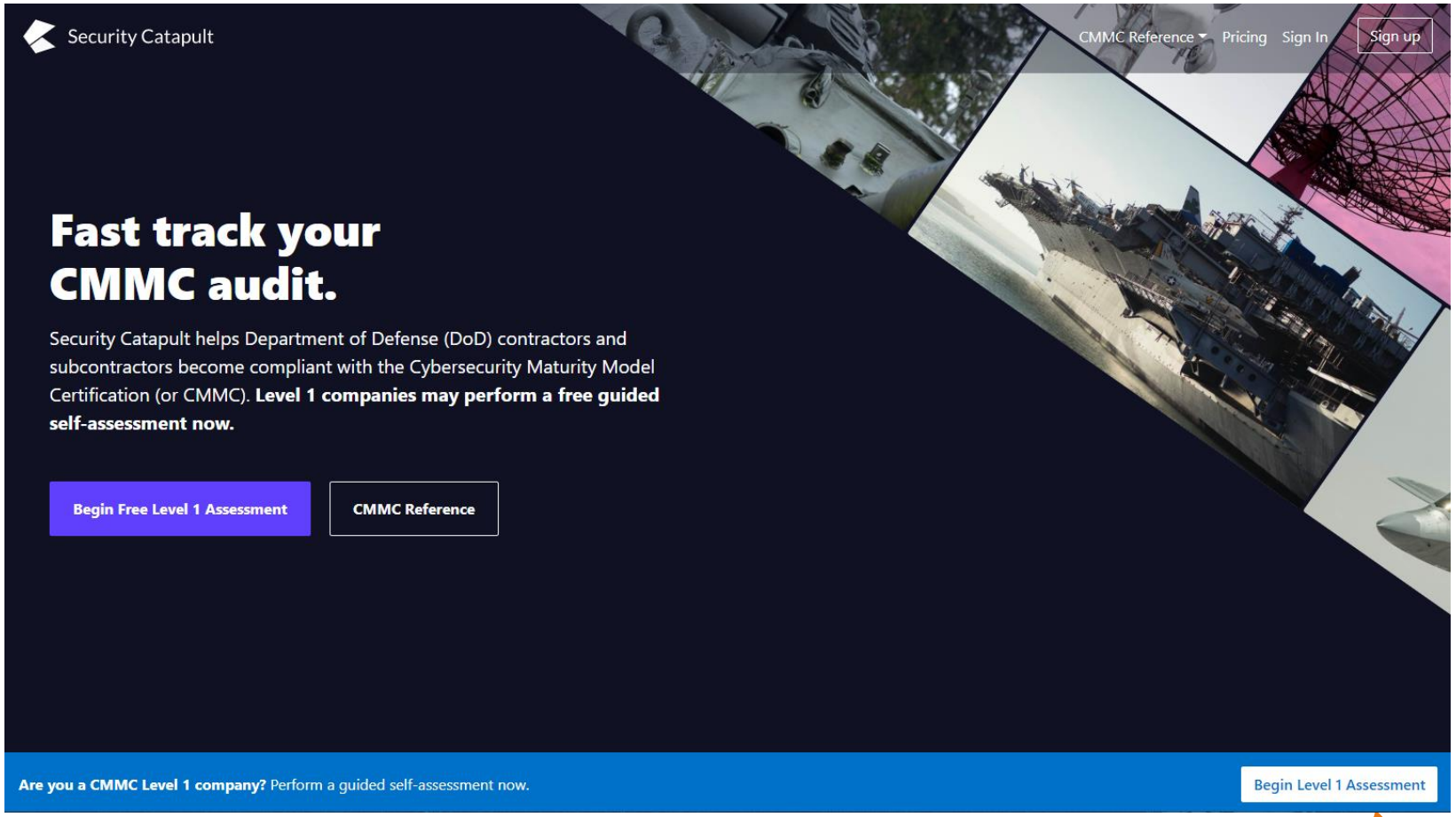
How We Can Help:

- Performing gap assessments
- Writing policies and security plans
- Training
- Call for a preliminary, no obligation consultation

MONARCH ISC
INFORMATION SECURITY CONSULTING

Where Do We Start?

Security Catapult™: Web-based self assessment tool



MONARCH ISC
INFORMATION SECURITY CONSULTING

Q&A

Questions?

MONARCH ISC
INFORMATION SECURITY CONSULTING

How to Get in Touch

Saco, ME
Telephone: 207-808-0472
Joe Kurlanski, CISSP® HCISPP®
President
Monarch Information Security Consulting, LLC
Email: joe@monarchisc.com

www.monarchisc.com
catapult.boldcoastsecurity.com

MONARCH ISC
INFORMATION SECURITY CONSULTING