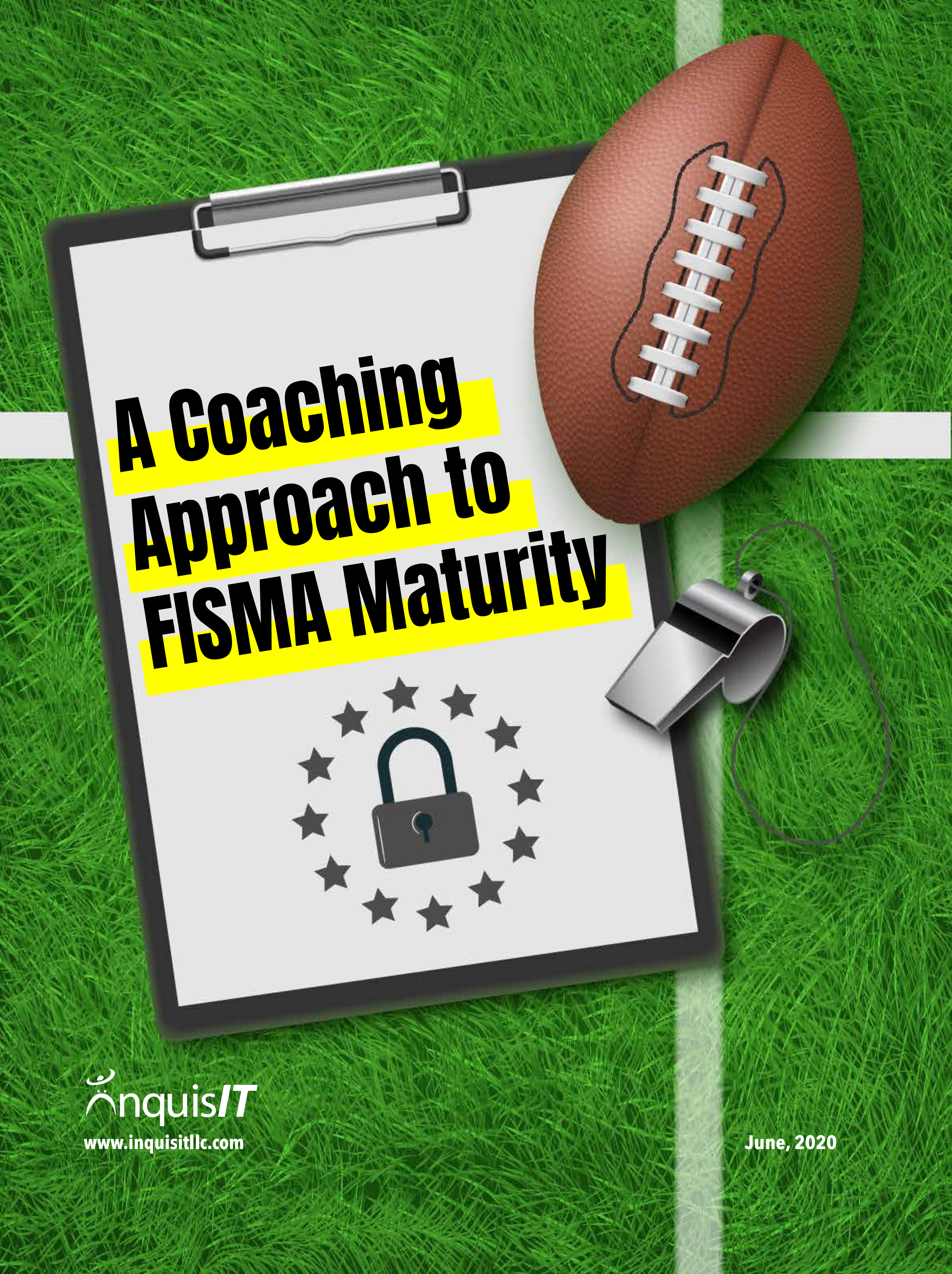
A Coaching Approach to FISMA Maturity



InquisIT

www.inquisitllc.com

June, 2020

INTRODUCTION

There are two sentences federal agency directors and business leaders never want to hear from their information technology departments: "we've been hacked" and "we failed our audit." They prefer to be focused on accomplishing their missions, which may include supporting such tasks as providing scientific solutions to address energy challenges, providing leadership on agricultural and natural resources, or supporting Warfighters on the front lines.

Whether it be a federal agency or contractor, the organization sees network availability as vital to mission accomplishment. However, unless organizations exist for the sole purpose of running networks, availability needs to support productivity while being seamless, transparent, and secure. In the federal sector, the Federal Information Systems Modernization Act (FISMA) adds a mandatory layer of additional complication to the team's tasks with routine compliance audits. Like any other team sport, **FISMA success starts with great coaching.**

FISMA compliance is hard. It is an expensive process, time-consuming, and often tedious. Every organization involved in federal government already knows this. For organizations looking to mature their programs, the below focus areas can help get you on the right track to coaching your team to FISMA victory.

FISMA IMPLEMENTATION PROJECT: NIST

"The E-Government Act (Public Law 107-347) passed by the 107th Congress and signed into law by the President in December 2002 recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA) requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other sources.

The Federal Information Security Modernization Act of 2014 amends the Federal Information Security Management Act of 2002 (FISMA) provides several modifications that modernize Federal security practices to address evolving security concerns. These changes result in less overall reporting, strengthens the use of continuous monitoring in systems, increased focus on the agencies for compliance, and reporting that is more focused on the issues caused by security incidents.

FISMA, along with the Paperwork Reduction Act of 1995 and the Information Technology Management Reform Act of 1996 (Clinger-Cohen Act), explicitly emphasizes a risk-based policy for cost-effective security. In support of and reinforcing this legislation, the Office of Management and Budget (OMB) through Circular A-130, "Managing Federal Information as a Strategic Resource,"1 requires executive agencies within the federal government to:

- *Plan for security*
- *Ensure that appropriate officials are assigned security responsibility*
- *Periodically review the security controls in their systems*
- *Authorize system processing prior to operations and, periodically, thereafter."*

[1] FISMA Implementation Project. National Institute for Standards and Technology (NIST). https://csrc.nist.gov/projects/risk-management/detailed-overview

START WITH THE RIGHT GAME PLAN

In the federal world, all roads for security compliance lead back to NIST. The several voluminous documents in the 800 series of Special Publications[2] contain all the answers to the test (audit). Established federal frameworks like RMF point back to NIST SP 800-30, 800-37, 800-39, 800-53, and 800-137, among others. For an idea of size, NIST SP 800-53 Rev. 4 weighs in at a hefty 462 pages! Due to the unique threats they face, the Department of Defense (DoD) follows DoDI 8510.01[3] RMF and all supporting documentation instead of the NIST series. Regardless, these will be essential documents to bring along for the process. Consider supplementing with a compatible and condensed framework that can serve as a sort of "CliffNotes", especially when it comes to getting the team to quickly rally around the process.

The nonprofit Center for Internet Security (CIS)[4] maintains a list of "Critical Security Controls" - twenty prioritized groups of controls that help manage risk with the greatest impact based on common threat scenarios. These are further broken into implementation groups, roughly analogous to organizational size or data criticality. Start at Control 1, work through it and move to Control 2 and so on. Schedule these as mileposts for a quick sanity check to spotlight what the organization might be missing from a more monolithic framework.

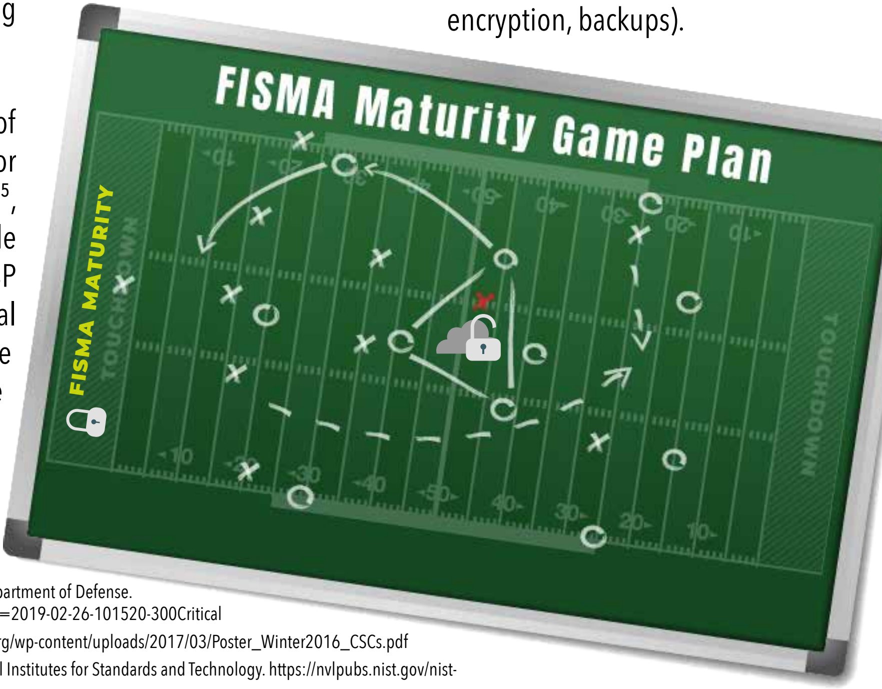
Another good framework, intended for operators of critical infrastructure, is the NIST "Framework for Improving Critical Infrastructure Cybersecurity"[5], released in 2018. At 55 pages, it's a manageable document with mappings directly to NIST SP 800-53 controls, among others. Don't let the "critical infrastructure" part of the title get in the way. The NIST CSF is a solid framework which is compatible with industry, and easily adapted to anything from a corner store to a nuclear power plant.

All good coaches have a game plan and can distill it to something the whole team can execute on quickly. Think of it as becoming the team's playbook, getting the necessary information to the right players without overwhelming them. It will require some creative thinking. Starting the special teams out with shorter guides that point in the right direction can focus them on the task of winning.

"I" STANDS FOR INFORMATION

Organizations are often quick to identify support systems such as domain controllers or network gear as their most critical technology assets. This is understandable due to their function, but flawed in the grand scheme of things. When we get to brass tacks, FISMA is all about protecting information. Securing servers and equipment is only a part of the puzzle.

With this "protect the Information" paradigm in mind, look around at other systems and identify the information that is most critical to the organization. While FISMA (and most information security practice) tends to place emphasis on confidentiality, remember that the integrity of information is something that the organization absolutely cannot function without. Identify this information and build defenses accordingly (e.g. data at rest encryption, backups).



[2] NIST Special Publication 800-series General Information. National Institute for Standards and Technology. https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information

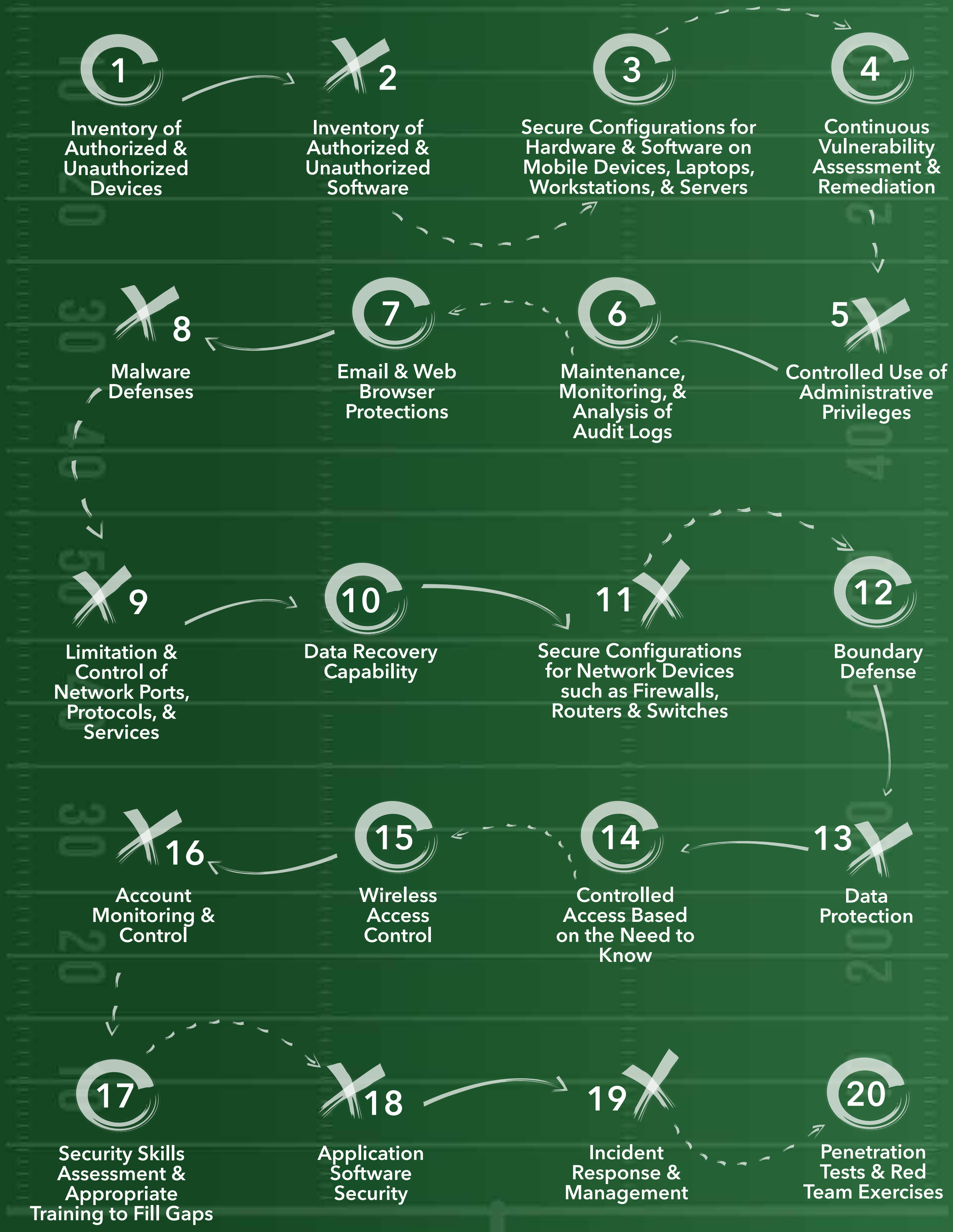
[3] Risk Management Framework (RMF) For DoD Information Technology (IT). (207) Department of Defense. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf?ver=2019-02-26-101520-300Critical

[4] Security Controls. (2016) Center for Internet Security (CIS). https://www.cisecurity.org/wp-content/uploads/2017/03/Poster_Winter2016_CSCs.pdf

[5] Framework for Improving Critical Infrastructure Cybersecurity. (April, 2018). National Institutes for Standards and Technology. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

AnquisIT

CIS "CRITICAL SECURITY CONTROLS" PLAYBOOK



1 Inventory of Authorized & Unauthorized Devices

2 Inventory of Authorized & Unauthorized Software

3 Secure Configurations for Hardware & Software on Mobile Devices, Laptops, Workstations, & Servers

4 Continuous Vulnerability Assessment & Remediation

5 Controlled Use of Administrative Privileges

6 Maintenance, Monitoring, & Analysis of Audit Logs

7 Email & Web Browser Protections

8 Malware Defenses

9 Limitation & Control of Network Ports, Protocols, & Services

10 Data Recovery Capability

11 Secure Configurations for Network Devices such as Firewalls, Routers & Switches

12 Boundary Defense

13 Data Protection

14 Controlled Access Based on the Need to Know

15 Wireless Access Control

16 Account Monitoring & Control

17 Security Skills Assessment & Appropriate Training to Fill Gaps

18 Application Software Security

19 Incident Response & Management

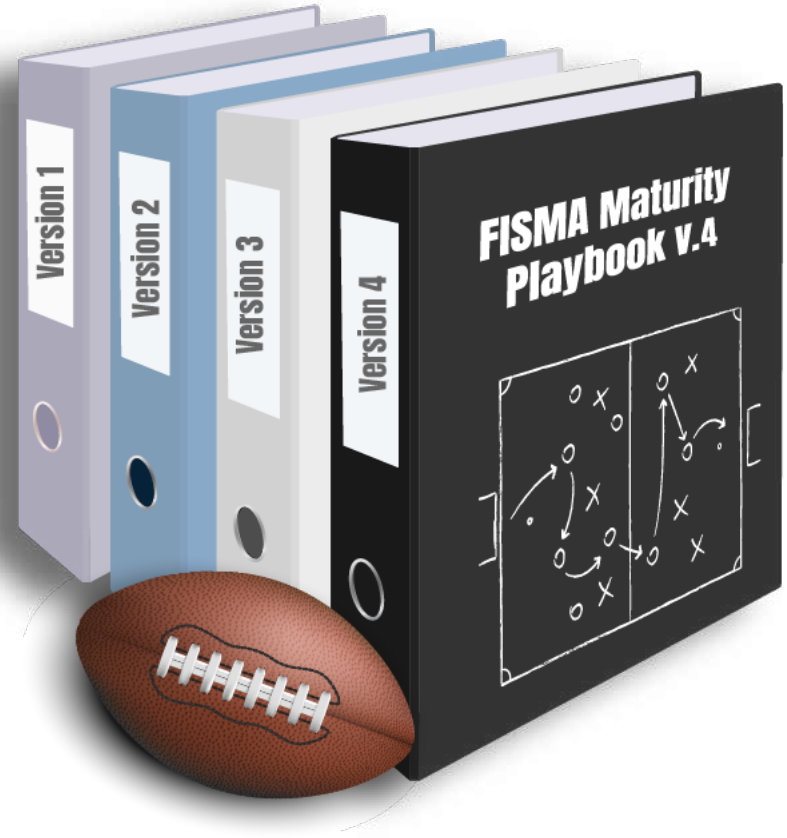
20 Penetration Tests & Red Team Exercises

CISO: "COACHING" INFORMATION SECURITY OFFICERS

Organizations that put the heavy lifting of FISMA compliance on the CISO's shoulders and leave it there are set up to fail. **Successful FISMA compliance is a team sport and the CISO will need to be an effective coach who pulls the necessary talent into special teams from across the organization.**

Since FISMA is more about the information than the technology, stakeholders from all over the organization must be engaged to achieve FISMA success. For example, the finance team will have people who know more about the critical information they process and its dependencies than any other department. These production centers will know what their own unique needs are to operate, and what houses the data they can't live without (e.g. share drives, databases). Ultimately, the CISO will bring the right executive decision-makers to the table to collaborate and decide to prioritize.

Finally, the Coach will bring all of the players back on to the field to rehearse plans. This ensures that the plans will work when called upon. Backups will be restored to ensure integrity. Virtual Private Network concentrators will be tested to handle emergencies that require employees to work remotely. Such tests may be inconvenient, so it takes a good coach to make everyone show up for practice when there are seemingly better things to do.



UPDATE THE PLAYBOOK

Having run through the foundational framework, identified critical information, and appointed a coach to lead the process, the organization now needs an updated plan to push forward. The plan will identify budgeted funding that reflects the priorities and capacity of the organization, dates to achieve specific goals, and a date to reconvene key members of the team to reevaluate.

DEVELOP & UPDATE DOCUMENTATION

FISMA requires documentation. Tons of documentation. Indeed, impervious technical controls, while admirable, are still a FISMA fail without documentation. The reason goes beyond mere bureaucracy; mature organizations ensure their processes are transferable, scalable, and repeatable. The only way to ensure this is to document those processes so the next person can pick up the torch.

In addition to the policy and procedure documentation, **FISMA requires accurate documentation and timely reporting of events and system changes.** Rare indeed is the IT professional who enjoys writing reports; it's easier to make a required change and move on to the next problem that needs to be solved. Having easy to use forms, templates, or service management systems (e.g. ServiceNOW) available to document changes improves the likelihood that your teams will be able to retrace their steps in the event of an issue.

TUNE-IN WITH YOUR SIEM

Few coaches can play every position on a given team; they rely on the players to swing bats, catch footballs, make free throws, and carry batons across finish lines. Good coaches motivate teams to succeed by clearly defining what needs to be done.

FISMA requires continuous monitoring. This requires retaining logs, which are useless unless someone is actively looking at them. Additionally, production networks have systems that generate millions of events which may consume precious network bandwidth. Storing logs consumes volumes of storage space, and this comes at a cost. Backing up stored logs only adds to that cost, all to support something that no one is ever looking at!

Put logs to use. Instead of just storing logs, feed them to a Security Information and Event Management System (SIEM)[6] and begin tuning to identify important events and reduce noise. With proper tuning and time, anomalous events will stand out and improve detection capabilities for events that would have been missed with manual log analysis.

On the most basic level, the SIEM should look for uncommon but interesting Windows events. For example, the below six events[7] can keep you ahead of potential malicious activity :

- New Process Executed (4688)
- Account Logged In (4624)
- Share Accessed (5140)
- Windows Firewall Network Connection by Process (5156)
- Service Added to the Endpoint (7045)
- File & Registry Auditing (4663)

Each of these requires some additional granularity in event capture configuration or at the SIEM to clean up noise. At minimum, these represent a good starting point for using the SIEM to generate FISMA artifacts. The addition of network security monitoring allows traffic event correlation to endpoint events.

[6] **To learn more about SIEM, read our white paper "Extending a Security Team through Security Information & Event Management (SIEM)"** https://www.inquisitllc.com/wp-content/uploads/2020/05/Extending-a-Security-Team-through-SIEM.pdf

[7] Gough, M. (2015). Finding Advanced Attacks and Malware With Only 6 Windows EventID's. Splunk. https://conf.splunk.com/session/2015/conf2015_MGough_MalwareArchaelogy_SecurityCompliance_FindingAdvnacedAttacksAnd.pdf

BREAK THINGS

Organizations that put controls in place but don't test them cannot be sure that the controls are working as intended.

Oftentimes there are holes, workarounds, and backdoors of which your team may or may not have awareness. Recruit them to begin identifying issues through vulnerability assessments. Ask, "if you had to get into X information, how would you go about it?" Consider rewards for solutions and encourage creative thinking.

Consider running monthly vulnerability scans, quarterly web application and database vulnerability scans, and annual penetration assessments. This can spotlight those areas that the local defenders can't pick up.

Recognize that the operators of the network are likely confident in certain controls, and either won't think to test them beyond verifying their existence or may not be sure how to test them at all. At this point, bringing in a third party for penetration testing is highly encouraged.

EMBRACE CONTINUOUS IMPROVEMENT

All of these steps represent a cycle. **No FISMA audit will ever end with a perfect score.** There will be problems that require funding to solve. There will be requirements that, if implemented, would break a business process or violate a still-in-force legacy system. **Develop and maintain a Plan of Action & Milestone (POA&M) program across your organization for such situations, and have the security team find ways to implement compensating controls.**

Accept that there will always be something that an evaluator finds that got missed. Use this as part of your process of continuous improvement, add it to the lessons learned, acquire what is necessary, and go at it again.

CONCLUSION

FISMA audits can be stressful for even the most prepared organization. A good roadmap, the right priorities, and solid leadership are key to success. Implementing a clear plan and executing to completion are critical to your organization's program maturity. Leverage timely, accurate documentation and reporting capabilities wherever possible for enhanced visibility. Be proactive, actively seek out vulnerabilities in your systems and addressing them. Such steps will go a long way to improving the posture of any organization, from the rookie to a seasoned veteran. A good coach can build a game plan that brings the whole team to victory, always improving, and ready for the next round.