



GUIDANCE NOTES ON

THE APPLICATION OF CYBERSECURITY PRINCIPLES TO MARINE AND OFFSHORE OPERATIONS

ABS CyberSafety™ VOLUME 1

SEPTEMBER 2016

**American Bureau of Shipping
Incorporated by Act of Legislature of
the State of New York 1862**

**© 2016 American Bureau of Shipping. All rights reserved.
ABS Plaza
16855 Northchase Drive
Houston, TX 77060 USA**

Foreword

ABS recognizes that automation methods – and increasingly, autonomy – have penetrated nearly all aspects of shipboard and platform systems. Because these systems control multiple aspects of asset, ship or platform operations, they become integral parts of system and operational safety.

ABS supports our community by compiling best practices, deriving new methods, and developing the standard for marine and offshore cybersecurity in a commitment to safety and security of life and property and preservation of the environment.

This document is Volume 1 of the ABS CyberSafety™ series. It provides best practices for cybersecurity, as a foundational element of overall safety and security within and across the marine and offshore communities. The best practices are meant to provide insights for operations, maintenance and support of cyber-enabled systems.

These Guidance Notes have been updated to align with Volume 2 of this series, *ABS Guide for Cybersecurity Implementation for the Marine and Offshore Operations – ABS CyberSafety™ Volume 2*. It has been expanded to reflect the full set of 37 Capabilities that define competencies for the ABS CyberSafety™ environment.

These Guidance Notes become effective on the first day of the month of publication.

Users are advised to check periodically on the ABS website www.eagle.org to verify that this version of these Guidance Notes is the most current.

We welcome your feedback. Comments or suggestions can be sent electronically by email to rsd@eagle.org.

11/15/2016 10:00 AM



GUIDANCE NOTES ON

THE APPLICATION OF CYBERSECURITY PRINCIPLES TO MARINE AND OFFSHORE OPERATIONS

ABS CyberSafety™ VOLUME 1

CONTENTS

SECTION 1	General.....	1
1	Objective	1
2	Application	1
3	Cybersecurity	1
4	Definitions	2
SECTION 2	Cybersecurity Program Development.....	3
1	Introduction	3
2	Intersection of Cybersecurity and Safety	3
2.1	Dependence on Software and Automation	3
2.3	Applicability	4
3	Best Practices	4
4	Structure for Best Practices	7
4.1	Basic Capability	7
4.2	Developed Capability	8
4.3	Integrated Capability	8
FIGURE 1	Basic Capability Set	5
FIGURE 2	Developed Capability Set.....	6
FIGURE 3	Integrated Capability Set.....	7
SECTION 3	Best Practices and the Application of Cybersecurity Principles to Marine and Offshore Operations: Basic Capability Set	9
1	Exercise Best Practices	9
1.1	References	9
2	Build the Security Organization	10
2.1	References	10
3	Provision for Employee Awareness and Training.....	10
3.1	References	11
4	Perform Risk Assessment.....	11
4.1	References	11

5	Provide Perimeter Defense.....	12
5.1	References	12
6	Prepare for Incident Response and Recovery.....	13
6.1	References	13
7	Provide Physical Security	14
7.1	References	14
8	Execute Access Management	14
8.1	References	15
9	Ensure Asset Management.....	16
9.1	References	16

SECTION 4 Best Practices and the Application of Cybersecurity Principles to Marine and Offshore Operations: Developed Capability Set..... 17

10	Perform Policy Management.....	17
10.1	References	17
11	Provide Standards and Governance.....	17
11.1	References	18
12	Provide and Guide Cybersecurity Hygiene.....	18
12.1	References	19
13	Gather and Use Threat Intelligence.....	19
13.1	References	19
14	Perform Vulnerability Assessment.....	19
14.1	References	20
15	Perform Risk Management	20
15.1	References	21
16	Provide Data Protection	21
16.1	References	22
17	Protect Operational Technology (OT).....	22
17.1	References	23
18	Perform System and Security Continuous Monitoring (SCM)	24
18.1	References	24
19	Plan for Disaster Recovery (DR).....	24
19.1	References	25
20	Provide Unified Identity Management.....	25
20.1	References	25
21	Perform System, Software, and Application Test	26
21.1	References	26
22	Perform System and Application Patch and Configuration Management	26
22.1	References	27
23	Execute Change Control as an Enterprise Process	27
23.1	References	27

SECTION 5	Best Practices and the Application of Cybersecurity Principles to Marine and Offshore Operations: Integrated Capability Set	28
24	Execute Capital Planning and Investment Control (CPIC)	28
	24.1 References	28
25	Implement Architecture Management	28
	25.1 References	29
26	Provide Secure Engineering	29
	26.1 References	30
27	Exercise Penetration Testing	30
	27.1 References	31
28	Build Forensic Analysis	31
	28.1 References	32
29	Enforce Privacy Management	32
	29.1 References	33
30	Provide Mobile Data Management	33
	30.1 References	33
31	Provide Certificate Management	34
	31.1 References	34
32	Exercise Communications Management	34
	32.1 References	35
33	Enforce Network Access Control	35
	33.1 References	35
34	Enforce Third Party Access Management	36
	34.1 References	36
35	Implement Secure Software Development	37
	35.1 References	37
36	Execute Security Test and Evaluation	38
	36.1 References	38
37	Provide and Use Audit	39
	37.1 References	39

This Page Intentionally Left Blank

Document ID: 123456789



SECTION 1 General

1 Objective (1 September 2016)

These Guidance Notes provide cybersecurity best practices and recommendations to marine and offshore organizations, and they are intended to enable members of the marine and offshore communities to take verifiable steps to protect an asset, its cyber-connected systems, its personnel, and its information from cyber intrusions. The overarching ABS cybersecurity guidance program provides these Guidance Notes within the overall program context of ABS CyberSafety™.

The principal objective of this document is to support the *ABS Guide for Cybersecurity Implementation for the Marine and Offshore Operations – ABS CyberSafety™ Volume 2* by providing a readable summary of the practices needed for CyberSafety. The best practices in these Guidance Notes provide the basis for the reader to understand the specifications, and the subsequent requirements, within each of the Capabilities listed in this document. In that way, Volume 1 serves as an introductory document for the more detailed Volume 2.

2 Application (1 September 2016)

These Guidance Notes apply to cybersecurity implementations for ships, platforms, vessels of any type, and support facilities, and the document supports a practical application of the engineering and operations of cyber-enabled systems in the marine and offshore environments.

Note: The general term “vessel” used throughout these Guidance Notes denotes a ship, a barge, an offshore asset or facility, or any other floating or fixed structure.

3 Cybersecurity

Security is a critical enabling function for an organization, company, agency or unit. Therefore, security is implemented to protect critical assets of all types, ranging from staff, equipment and facilities to computerized systems. Security implementations themselves are assets, requiring the same security protections that they in turn offer to the larger organization. Most Companies arguably understand the need for protecting and monitoring cyber-linked business support and control systems. Even so, the breadth and complexity of protecting such systems may present a daunting challenge to many organizations that do not have a comprehensive picture of cybersecurity.

Successful cybersecurity is the result of a complex series of related and interdependent work efforts that intersect so as to provide protections that are functional and enduring in the face of challenges presented by geography, technological evolution, and shifting human resource capabilities and deployment.

A thorough understanding of the protected Company, its supporting physical and intellectual assets, and the needs and capabilities of its people provides the foundation for a structured cybersecurity program. That security program expectedly changes and develops as it orders and prioritizes requirements, develops its capabilities, builds its functional capabilities, and aligns itself with the Company, its mission and its goals. Because every Company is unique in its needs, priorities and limitations, every security program is also unique in its protective functionality, sequence of areas protected, and protection timetables.

This document, “Volume 1: Cybersecurity”, of the ABS CyberSafety™ series, appreciates and accommodates the unique characteristics required to build and maintain a cybersecurity program. The Guidance Notes offer guidance that attempts to represent due care and due diligence in cybersecurity.

4 Definitions (1 September 2016)

Capability: The ability to execute a specified course of action. (Adapted from: CNSSI 4009, Joint Publication 1-02. Source: http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf)

CyberSafety: Guidelines and standards for computerized, automated, and autonomous systems that **seek to shape those systems to be** designed, built, operated, and maintained so as to allow only predictable, repeatable behaviors, especially in those areas of operation or maintenance that can affect human, system, enterprise or environmental safety. CyberSafety is required for the deterministic behaviors found in engineered functional assurance, and it includes software integrity management to manage technical risk in software-intensive systems.

ABS CyberSafety™: Measurable implementation of CyberSafety that tailors cybersecurity and systemic safety to assets in order to enable and encourage risk-based asset management as a systemic outcome. ABS CyberSafety™ will provide deterministic outcomes when implemented within managed environments that include appropriate processes, policies, system test and audit, and data management.

Cybersecurity: The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation. (Adapted from: CNSSI 4009, NIST SP 800-53 Rev 4, NIPP, DHS National Preparedness Goal; White House Cyberspace Policy Review, May 2009. Source: <https://niccs.us-cert.gov/glossary>)

Information Technology (IT): Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. (From: NIST SP 800-53 Rev 4 (glossary). Source: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>)

Operational Technology (OT): An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition (SCADA) systems used to control geographically dispersed assets, as well as distributed control systems (DCSs) and smaller control systems using programmable logic controllers to control localized processes. (Adapted from: NIST SP 800-53 Rev 4. Source: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>)

Smart Asset: Marine and offshore assets built with significant degrees of automated control of vessel or platform operations, system management and monitoring, and data communications. Automation provides labor-saving capabilities; augments human strength; augments human decision-making and error-checking processes; provides operational situational awareness; enables multiple simultaneous system control and management; and provides for controlled data storage. A Smart Asset may possess automated or autonomous processes that operate without routine human intervention.



SECTION 2 Cybersecurity Program Development

1 Introduction

ABS recognizes that automation is pervasive in shipboard and platform systems. Because automated systems control multiple critical aspects of marine and offshore assets, ship and platform operations, these systems are now subject to the same safety-related concerns as is any other critical vessel feature.

“Volume 1: Cybersecurity” addresses cybersecurity practices for systems, ships and platforms as part of the ABS CyberSafety™ series. Beginning with best practices, the series will help owners, operators and regulators to verify the various automated systems found at sea and ashore can neither cause harm to personnel, nor compromise system integrity or operations.

Cybersecurity is the first area to be addressed in building secure and safe systems. As the series matures and is implemented by ship and platform owners, operators and crews, additional products will be provided to support self-assessment, self-test, and self-audit. The series will provide test, data management, software assurance, automated systems (i.e., robotics and safety-critical systems) and autonomous system guidance and technical direction. Appendices to the ABS CyberSafety™ document series will provide strategy, policy, processes, and safety assessment tools, checklists and audit templates.

2 Intersection of Cybersecurity and Safety *(1 September 2016)*

2.1 Dependence on Software and Automation

The marine and offshore environments include pervasive information technology (IT), and extensive and growing numbers of cyber-physical systems (CPS). These systems provide labor multipliers to assist the captain and crew in operating the ship effectively and efficiently, providing machinery and ship controls, monitoring and alerting. Navigation, propulsion, ship control (maneuvering), system management, cargo management, and safety sensors and alarms – all supplement people and assist people while providing functions to keep people working and out of harm’s way. Both IT and CPS systems must operate as expected if they are to support the crews’ processes and procedures.

Ship and platform automated systems are now connected in ways never before considered. Crews, vessel operators, platform or facility managers, and original equipment manufacturers (OEMs) want remote access, greater on-station function, frequent reporting from sensors, and new types of data and functions. To support these requirements, many control systems are coupled via industry-standard communications and networking, interfaced to Internet-connected networks, and operated in multiple modes unanticipated at system design. The result is that general-purpose systems are frequently connected to special purpose process control systems, exposing control systems to security incidents that can have operational consequences.

A cybersecurity incident on a ship, on a platform, or within a facility, might result from system fault or failure, operator error or inaction, inadvertent conflicts in incompatible software, or deliberate malfeasance or malice. Any such incident may result in intrusion or malfunction in a general purpose network, resulting in a cascading failure that can spread into ship or platform CPS to cause unexpected consequences for any number of systems.

Because of system interconnections, a CPS failure might even cause ship-wide failures that can, in turn, affect the surrounding community and environment. It is the responsibility of mariners and seafarers to know their systems, know their interfaces, know how both work together, how they might fail, and the failure consequences.

Cybersecurity and software integrity management are both increasingly important to the broader understanding of our systems, our software, and our overall system safety. Cyber-enabled systems and gear are all around us. The security aspects of highly automated, integrated, computerized gear must be well understood, especially when considering the safety-related impacts of security on both individually controlled systems and linked systems.

2.3 Applicability

Cybersecurity, as envisioned and presented in this document, protects against both malicious and inadvertent sources. User error, accidents, hardware failures, software faults, or negligence must all be designed or allocated out of the system, in addition to designing out potential avenues of intentional attacks, with the goal of making the systems being protected resilient and safe for personnel, the ship or asset, and for the environment.

The objectives and/or implications of either inadvertent or malicious cyber-system faults, errors or attacks can vary widely. If malicious, system control is just one possible consequence of hostile actions. Data exfiltration and intellectual property theft are known potential risks. Use of a system as a “jumping off point” for other attacks, whether against other Company assets or against outside organizations, is another possible outcome.

Of equal importance, however, are the implications of user error or negligence, and either man-made or natural disasters on the information and control systems built into ships or at-sea assets. Far more opportunities for human error or inadvertent system faults present themselves in system operations than designers or builders expect; it is the training and documentation of processes and procedures that help insure against these categories of errors. For natural disasters, we plan for business continuity, designing resilience into systems, processes and assets.

The first step to improved cybersecurity is knowledge of the approaches developed and implemented by other practitioners in the field who have gained and shared valuable experiences and lessons learned. This document contains practical information that has been researched and vetted for application to the marine and offshore industries. It is a collection of best practices deemed to be useful both to novice specialists just beginning to establish cybersecurity programs, and to seasoned experts who want to review the best practices of others in order to continue improving their cybersecurity programs and implementations.

3 Best Practices (1 September 2016)

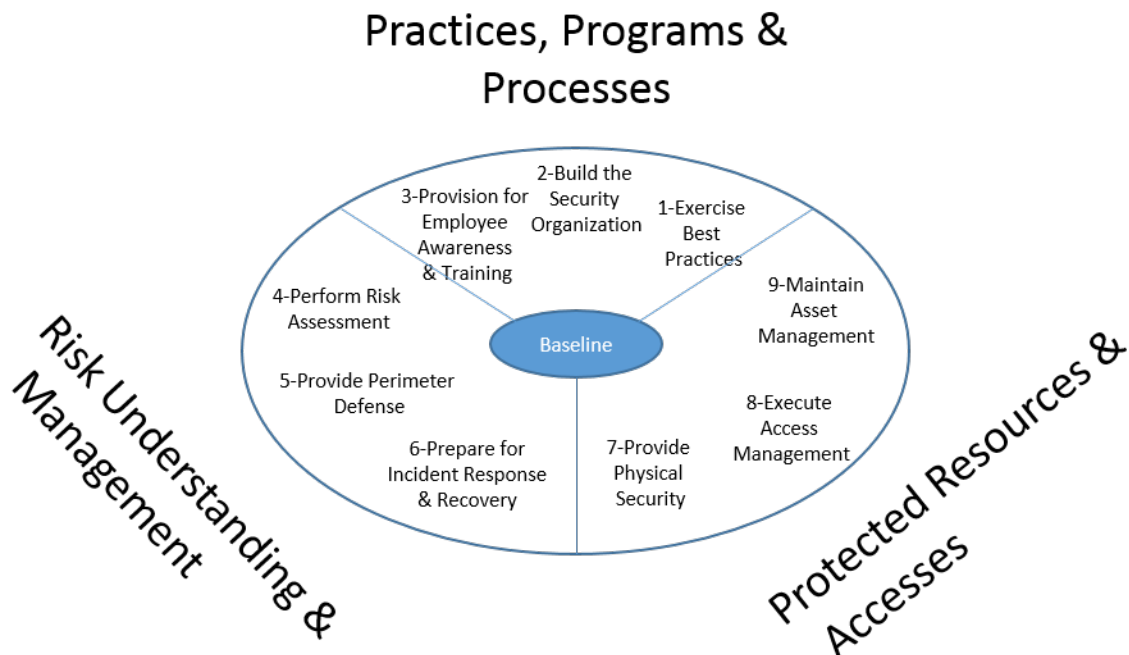
ABS CyberSafety™ is the ABS process for adding cybersecurity rigor to both the operational systems aboard ships and platforms, and to the linked business systems that support their missions. The best practices in these Guidance Notes will help the reader understand how to frame and prioritize cybersecurity work efforts in going about building rigor, security and safety into systems.

This volume concentrates on the establishment of Basic and Developed Capabilities that fully enable a cybersecurity work effort. In this context, a Capability is broad in that it includes people, systems, data, and processes. A Company builds these Capabilities incrementally based on security needs, staff competencies, available acquisition resources, and organizational maturity in cybersecurity.

Capabilities built according to this method become the Company's support framework for security controls, policies and procedures. The program laid out in this way becomes an overlay that can be used with any compliance framework's security controls, or it can be a measurable compliance set in its own right. The arrangement of the Capabilities is consciously structured to provide supportability and life cycle management inside the personnel structures built and maintained by the Company, for both cybersecurity and system safety.

Section 2, Figure 1 illustrates the most basic Capabilities that are required to build a cyber-safe program to support cyber-secure systems. At the core of the program are the baseline controls and tasks – the information technology fundamentals – commonly employed to support a business or operational (shipboard, offshore or port facility) system. Surrounding this baseline are Capabilities needed to shape an environment that is ready to sustain a robust cybersecurity program.

FIGURE 1
Basic Capability Set (1 September 2016)



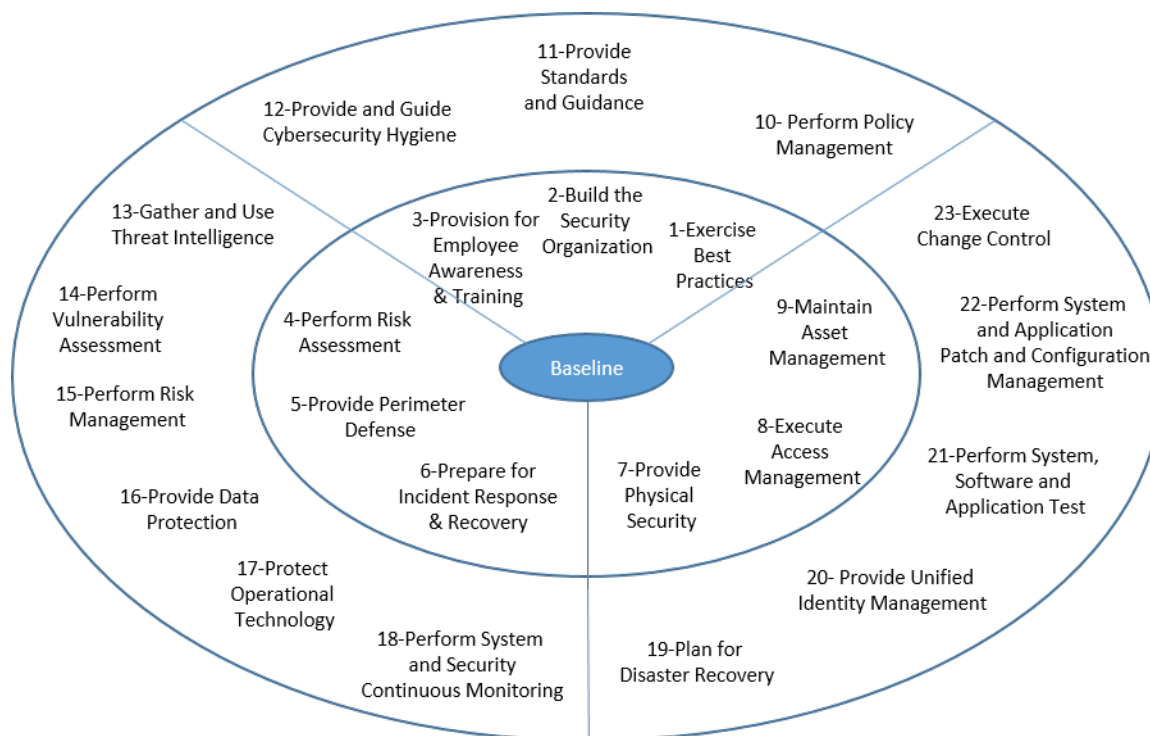
The nine Basic Capabilities shown should be developed and implemented within the **Company**, and should be evident as fully documented, employed, supported, and maintained.

These Capabilities are critical to establishing a viable cybersecurity program, and they are judged by ABS to be the minimum set required in order to evaluate, analyze, and provide a measurable initial status of cybersecurity in automated systems and their host organization(s). The nine Capabilities are arranged in more general divisions that can aid in organizing and understanding the functions, factors which may be more important in smaller, or less mature, **companies** that must be relatively more careful about expenditures and personnel assignments.

Capabilities are the primary elements supporting a cybersecurity program. Capabilities enable companies to perform complete cybersecurity tasks that are interrelated with other software and systems engineering tasks. Prioritization of the security tasks, and the Capabilities that enable those tasks, may change based on a **Company's** available resources for performing the tasks and its installed base of assets requiring protection. In support of those imperatives, "Volume 1: Cybersecurity" provides a way to approach prioritization in a scalable, measurable, and complete way.

Section 2, Figure 2 indicates how this cybersecurity program extends the foundational Basic Capability Set into a more functionally complete Developed Capability Set. These additional Capabilities build on the Basic Capability Set to provide both depth and breadth in the three functional divisions. The purpose of this layered approach is that it enables the builder of a cybersecurity program to select and implement Capabilities in a way that best satisfies the needs and constraints of the supported organization or asset.

FIGURE 2
Developed Capability Set (1 September 2016)

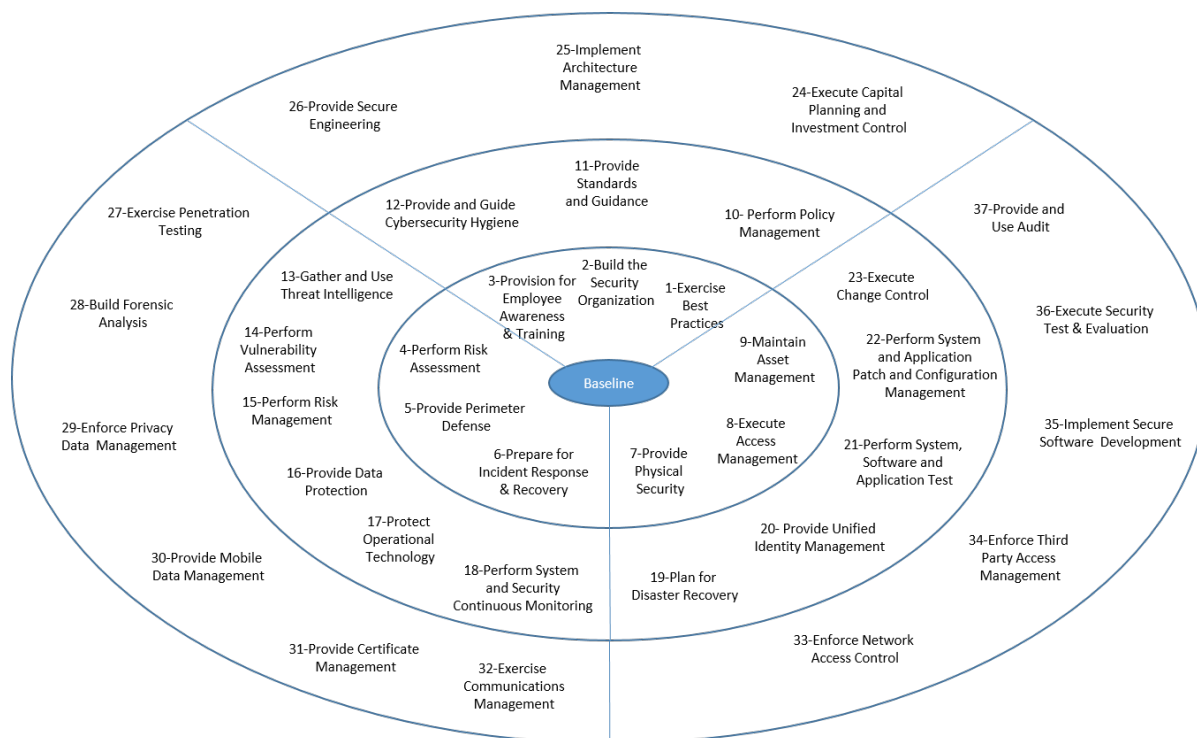


The outside layer of the Developed Capabilities Set provides relative completeness to a **Company** having a need, a level of maturity, and available resources to establish a well-formed cybersecurity system. A third set of capabilities provides guidance for a fully formed, highly capable cybersecurity system.

Section 2, Figure 3 presents the model fully, showing the Integrated Capability Set. This third set of components provides for capabilities needed to manage and operate combined task sets in a complex environment.

Single capabilities from the Basic or Developed sets can be self-contained. The Integrated set builds capabilities in the Company that require multiple derivative inputs to generate full value for the Company.

FIGURE 3
Integrated Capability Set (1 September 2016)



4 Structure for Best Practices (1 September 2016)

Below are the Best Practices that ABS associates with the layers of cybersecurity capabilities minimally needed to protect **companies, ships, and offshore assets**. These Best Practices are compiled from across multiple industries, multiple government reports, individual recommendations, and white papers.

Not all best practices fit every situation, operational context, or application; even so, the listed practices are primarily based on lessons learned by implementers that have paved the way in cybersecurity program development and can arguably enable a practitioner to stand up a functional cybersecurity program more rapidly and logically than would be possible without this or similar guidance

These Guidance Notes are organized as best practices and recommendations for each of the Capabilities shown in the preceding cybersecurity program graphics. The Basic Capability list deemed to be essential to a nascent program is provided first, followed by the Developed Capability list.

4.1 Basic Capability

1. Exercise Best Practices
2. Build the Security Organization
3. Provision for Employee Awareness and Training
4. Perform Risk Assessment
5. Provide Perimeter Defense
6. Prepare for Incident Response and Recovery
7. Provide Physical Security
8. Execute Access Management
9. **Maintain** Asset Management

4.2 Developed Capability

10. Perform Policy Management
11. Provide Standards and Governance
12. Provide and Guide Cybersecurity Hygiene
13. Gather and Use Threat Intelligence
14. Perform Vulnerability Assessment
15. Perform Risk Management
16. Provide Data Protection
17. Protect Operational Technology (OT)
18. Perform System and Security Continuous Monitoring (SCM)
19. Plan for Disaster Recovery (DR)
20. Provide Unified Identity Management
21. Perform System, Software and Application Test
22. Perform System and Application Patch and Configuration Management
23. Execute Change Control as an Enterprise Process

4.3 Integrated Capability

24. Execute Capital Planning and Investment Control
25. Implement Architecture Management
26. Provide Secure Engineering
27. Exercise Penetration Testing
28. Build Forensic Analysis
29. Enforce Privacy Data Management
30. Provide Mobile Data Management
31. Provide Certificate Management
32. Exercise Communications Management
33. Enforce Network Access Control
34. Enforce Third Party Access Management
35. Implement Secure Software Development
36. Execute Security Test & Evaluation
37. Provide and Use Audit

Each Capability section contains a series of identified recommendations and best practices that minimally satisfy the Capability, a short discussion of the section, and a list of references that are useful for further reading and understanding. *The Best Practices then flow forward into the capability implementation specifications in the ABS Guide for Cybersecurity Implementation for the Marine and Offshore Operations – ABS CyberSafety™ Volume 2.*

The Best Practices are set off from explanatory text and references by use of italic font to highlight the practices.