



Julie Hallett

# A Practical Guide to Cybersecurity in SAP®

- ▶ Cyber risk in the SAP landscape
- ▶ Cybersecurity risk management programs in SAP
- ▶ How to harden security
- ▶ Risk mitigation for threats

# Table of Contents

<b>Preface</b>	<b>9</b>
<b>1 Introduction</b>	<b>11</b>
<b>2 Cybersecurity defined</b>	<b>13</b>
<b>3 Using a security framework to manage risk</b>	<b>17</b>
3.1 What is a framework?	17
<b>4 Reconciling SAP cybersecurity to frameworks and regulatory compliance requirements</b>	<b>29</b>
4.1 Framework and guideline types	29
4.2 Steps of a compliance project	31
<b>5 Leveraging the NIST CIS Controls version 7.1 framework for SAP</b>	<b>39</b>
5.1 Reconciling SAP Cybersecurity to the NIST CIS Controls	39
<b>6 Cybersecurity threats to SAP</b>	<b>55</b>
6.1 Historic threats—users, customization, no post-go-live cleanup, no archiving	55
6.2 The new and emerging threat matrix for SAP	59
6.3 Hackers—the most common threats and abuses	61
<b>7 Implementing cybersecurity risk management in SAP</b>	<b>67</b>
7.1 Managing the new, combined level of risk	67
7.2 Connections, users, security notes, and SAP penetration testing	68
7.3 Leverage SAP Access Control to manage risk	69
7.4 Security role rebuild	69
7.5 SAP Security Notes	69
7.6 Cloud vendor review, mobile device policy and management	69
7.7 Tools to monitor compliance	70

<b>8</b>	<b>Policy and education</b>	<b>73</b>
8.1	Security policy, standards and procedures	73
8.2	Applying policy to SAP	77
<b>9</b>	<b>Governance, risk, and compliance</b>	<b>81</b>
9.1	Overview	81
9.2	Governance of cloud or hybrid cloud environments	82
9.3	Leveraging SAP GRC Access Control to monitor security compliance	85
<b>10</b>	<b>SAP Security Notes</b>	<b>87</b>
10.1	Security Notes review process	87
10.2	Vulnerability scoring decision matrix	90
<b>11</b>	<b>Communication security</b>	<b>95</b>
11.1	Remote Function Call (RFC)	95
11.2	Internet Connection Framework (ICF)	97
<b>12</b>	<b>Critical authorization objects</b>	<b>101</b>
<b>13</b>	<b>Information security for data at rest</b>	<b>107</b>
13.1	Types of data	107
13.2	Threats and risks	108
13.3	Tools and techniques for protecting data at rest	111
13.4	Cybersecurity program integration	114
<b>14</b>	<b>Preparing for new technology</b>	<b>117</b>
<b>15</b>	<b>Audit preparation</b>	<b>119</b>
15.1	Framework	119
15.2	Artifacts	119
15.3	Monthly checks	120
15.4	Automated process checks	120
15.5	User access reviews	121
15.6	User change history	121
15.7	Non-administrative user lockouts	122

<b>16 Risk management</b>	<b>123</b>
16.1 Mitigations	123
<b>17 Conclusion</b>	<b>125</b>
<b>18 Appendix A: SAP Audit Logs</b>	<b>127</b>
<b>A The Author</b>	<b>143</b>
<b>B Index</b>	<b>144</b>
<b>C Disclaimer</b>	<b>148</b>

## 2 Cybersecurity defined

**Cybersecurity is not a simple term. It is a concept, program, and process that encompasses data security as a whole. Understanding the holistic nature of cybersecurity will help to develop the process to bring SAP® into a cyber/data security program.**

*Cybersecurity* has been a major buzzword over the last few years, and will continue to be so in the future. It refers to the technologies, processes, and practices designed to protect networks, computers, programs, and data from attack, damage, and unauthorized access, as defined by the U.S. National Institute of Standards and Technology (NIST). It is not simply another name for security, it is the holistic program that wraps around multiple layers of security, compliance, policy and education.

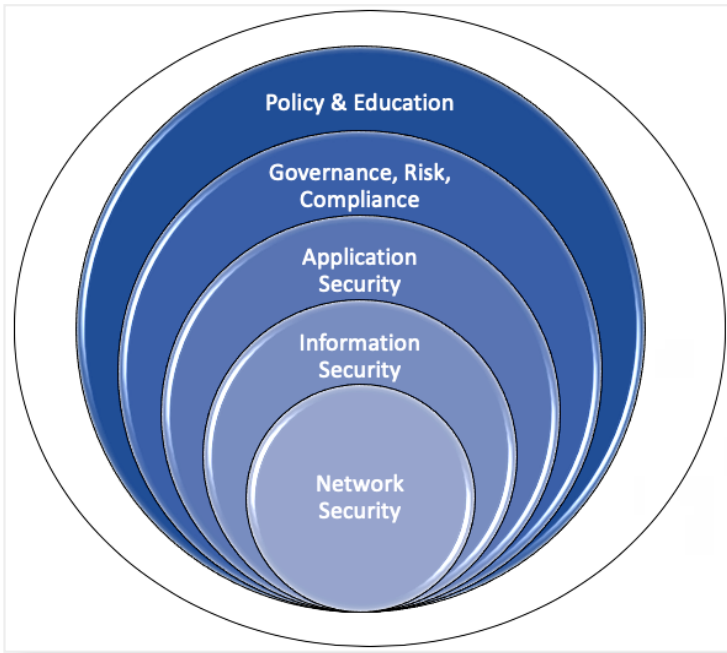
### Stop hackers at the network perimeter



Cybersecurity is much more than a way to stop hackers at the network perimeter. It incorporates all aspects of data security, including the largest threat to security—people: employees, contractors, and customers.

A *cybersecurity program* is a holistic processing of requirements and tasks across all layers (see Figure 2.1). It results in a communications chain that manages change across all areas of the IT organization. The goal of the program is to ensure each layer takes into account the other areas impacted by new and emerging threats, and to change implementation.

Creating a holistic data security plan requires a well-thought-out and planned cybersecurity program. In this diagram, the layers of the program are nested and sized according to their importance, level of potential risk, and difficulty to manage. *Network security* receives the most publicity in cybersecurity discussions, but it only plays a small part and depends on the other layers from the perspectives of education, execution, and governance.



*Figure 2.1: Elements of a cybersecurity program*

*Policy and education* is the largest and most complex layer of a cybersecurity program. Definition, socialization and enforcement of policy has legal implications across the entire organization. Security education often requires customization for company divisions, job levels, departments and risk levels, according to the data being managed. This includes the delivery methods for the curriculum, enforcement of education, and recertification on an annual basis. Once employees are educated, regular updates and education about new threats need to be delivered to each employee. The policy and education layer is the foundation of all governance and compliance efforts, applications, information and network security.

*Governance, risk and compliance* in the cybersecurity program is not a reference to the SAP GRC module (also called Governance, Risk and Compliance). Here, it refers to the processes of managing overall risk to the information, data, intellectual property, and systems that belong to a company. This includes monitoring and enforcing policy, education requirements, threat identification and response, business continuity planning and disaster recovery.

Managing compliance to regulatory requirements for the corporate location and business space means keeping up with all the latest regulations such as the European Union General Data Protection Regulation (GDPR), the NIST CIS (Center for Internet Security) Controls, and the Cybersecurity Maturity Model Certification (CMMC) that are currently being implemented by the US Government as of 2020, as well as many other regulation and certification requirements. The requirements of these regulations permeate through all layers of a cybersecurity program generating new policy, education, application and information security requirements and classifications as well as network security processes.

*Application security* includes office automation applications, access to network shared drives and data stores, business automation applications, human resources applications, research and development, and many others. Each application has access to data through specific data-storage locations. Access to display or maintain that data needs to be given, while also being careful to provide only the minimum amount of access needed for task requirements. Many companies default to a model where they give their users access to everything they might need at any point in time in order to reduce future access requests and minimize interruption to task execution. Access models are often copied from one group to the next without carefully considering data confidentiality. Designing and implementing application security is time and resource intensive; however, remediation of security after an incident, or for regulatory requirements is much more difficult and can risk business continuity.

*Information security* includes classification of data into confidentiality tiers. The review and identification of data that is to be restricted is dictated to some extent by regulatory and legal requirements. This includes human resources (HR) data, personally identifiable information (PII), protected health information (PHI) and some company financials. Using this as the only restrictions on corporate information creates risk to the data, thereby impacting a company's trade secrets such as customer lists, price lists, suppliers and supplies, product bills of materials, drawings and assembly details, and new product development. These could be mismanaged and left available to hackers. It is at this level of detail that the intersection between application and information security becomes critical. Unclassified information that is left available to many applications is classified as potential risk. If that data is saved by an employee on an unsecured internet drive (in order to work on it elsewhere), the situation changes from a potential risk to an actual risk, unknown and unmanaged.

These different layers can either reduce or create risk at the network security layer. A breach of policy due to lack of education can introduce new, emerging, or *zero-day* threats to the network. A zero-day threat is a vulnerability that has not previously been discovered or exploited. Zero-day means it is the very first time the vulnerability has been exploited by a hacker. The more access the users have across applications and information stores, the more areas a *threat actor* has to act upon. A threat actor is any person, entity or code that exploits risks or attacks systems. This could include information theft, the planting of malicious code, or the implementation of a robot/bot network application that can launch attacks against other internal targets, external companies, or entities from within the corporate network perimeter.

### The use of Shadow IT



Another example of how all the different layers of a cybersecurity program work together to secure corporate data and assets would be the use of *Shadow IT*—the implementation of a technology solution outside the control of the IT department. This occurs when an internal business team decides to employ a cloud service provider to do data enrichment or other services.

When groups or departments decide to implement an application and access to it, without the knowledge or participation of the company's IT team, the standard information technology policies and processes are circumvented, which is a breach of protocol that introduces multiple layers of risk. The use of this service now introduces new data, network and access management risks when it is not in a managed or approved process. This includes the risk that a terminated employee is not removed from their company's online access. If the user is not removed, they will still be able to access the data, and the credentials of that user are then compromised (especially if users are using the same password everywhere). This creates a network penetration risk. Additionally, issues encountered by the service provider are now risks to the company as a whole.

The connection and communication of the five layers of a cybersecurity program are critical for creating a secure, informed technology environment and for managing risk.



# 3 Using a security framework to manage risk

A framework is a tool used to identify the right questions to ask, and to understand how to organize that information into manageable standards.

## 3.1 What is a framework?

A framework is a set of guidelines laid out to create standardization across processes. Frameworks are the tools used to implement standards. The terms *frameworks* and *standards* are often used interchangeably. For the purposes of this chapter, we will use them separately with their common definitions:

- ▶ *Framework*—a basic structure or system of rules underlying a system; a concept that facilitates decision making
- ▶ *Standards*—a rule, principle, technique, process or template designed to provide consistency to planning, development, operation, implementation and governance

A framework is the foundation of questions that guide the creation, understanding, and education of standards and policies. Standards can be self-governing, but the framework provides high level governance to ensure the standards are being met and monitored. Where things get tricky is when there are different frameworks that govern different types of data.

### Frameworks are tools to create structure and stability



Frameworks provide a structured set of topics to use to evaluate a system or software. They can be used for any hardware, software, network or data management process to create stability and security.

# B Index

## A

- Activity 46
- Actual risk 85
- Antimalware 71
- Antivirus 71
- APIs 61
- Application Programming Interfaces (API)s 95
- Application security 15
- Archiving 59
- Articles 22
- Attack surface 59
- Audit artifacts 119
- Audit controls 73
- Auditing 119
- Authentication Bypass 64
- Authorization stacking 57
- Automation 22

## C

- Capabilities 25
- Certification 25
- Change management 79
- Chapter 22
- Child Role 80
- Clickjacking 93
- Cloud 82
- Cloud Services 69
- CMMC 19, 24
- CMMC Level 25
- COBIT 2019 19
- Code base 90
- Code Injection 63
- Code Vulnerability Analysis 72
- Command Injection 64
- Common Vulnerability Scoring System 35
- Compartmentalizing 60

- Confidential Data 19
- Confidentiality 107
- Content Spoofing 93
- Continuous diagnostics and mitigation 22
- Controls 21
- Copy back, 107
- Credentials 16
- Critical transactions 85
- Customer masters 107
- Customizations 58
- CVSS score 88
- CVSS Score 88
- Cyber Hygiene 24
- Cybersecurity Maturity Model Certification (CMMC) 15

## D

- Data at rest 107
- Data at Rest 108
- Database sharing 61
- Data classification 49
- Data Controller 23
- Data integrity 107
- Data in Use, Data in Motion 108
- Data Processing 23
- Data Processor 23
- Data Subject 23
- Dependencies 87
- Derived role 69
- DIB 24
- Directory Traversal 62
- Domains 25

## E

- EAM 69
- Early Watch Alerts and Reports 114

EarlyWatch Reports 72  
Encrypted container 70  
Enterprise Threat Detection 71  
Environment impact 88  
Escalation of privileges 57  
European Union General Data  
Protection Regulation (GDPR)  
15

## F

Field Masking 72, 114  
Financial Data 18  
FIORI 41  
Framework 17

## G

GDPR 19, 22  
Governance, Risk and Compliance  
14  
Governance, Risk, and Compliance  
81  
Guidelines 73

## H

HANA 41  
Hardcoded Credentials 64  
HIPPA 19, 84  
Hybrid cloud 82

## I

IaaS 59  
IDaaS 59  
IFC\_VALUE 46  
IGs 21  
Information Disclosure Vulnerability  
63  
Information security 15  
Intellectual Property (IP) 18  
Internet Communication Framework  
(ICF) 95

## M

Mainentry 13, 14  
  Prioritization 21  
  SSAE 16 70  
Malicious code 16  
Malware 65  
Master data 107  
Master Data 19, 107  
Maturity Model 25  
Measurements and Metrics 21  
Missing Authorization Check 62  
Mitigating 81  
Mitigating control 85  
Mitigating controls 124  
Mobile device management  
  software 60  
Mobile Device Management suite  
70

## N

Nation State Actors 108  
Need to Know access 49  
NetWeaver Business Client  
(NWBC) 41  
New, emerging, or zero-day threats  
16  
NIST CIS Controls 15, 20  
NIST CIS CONTROLS 19

## O

Offense informs defense 21

## P

PaaS 59  
Parent role 80  
Penetration testing 71  
Penetration Tests and Red Team  
  Exercises 53  
Personal Data 23

Personally Identifiable Information (PII) 18  
Phishing 93  
Policies 73  
Portal 41  
Potential risk 85  
Practices 25  
Principle of least privilege 49  
Procedures, 73  
Processes 25  
Proliferation of risk 90  
Protected Health Information (PHI) 18

## R

Recitals 23  
Remote Function Call (RFC) 45, 95  
RFC 89  
RFCDEST 46  
RFC Name 46  
RFC Type 46  
RFCTYPE 46  
RFC Vulnerabilities 89  
Risk assessment 123  
Risk management 123  
Risk Mitigations 123  
Risk scoring 88  
Robot/bot network 16  
role-based access control 51

## S

SaaS 59  
SAP\_ALL 68, 121  
SAP HostControl 68  
SAP Message Server 68  
SAP Microsoft Management Console 68  
SAP\_NEW 68  
SAP Notes for Security 43  
SAProuter 48

SAP Router 68  
SAP Security News 69  
SAP Security Notes 68  
SAP Solution Manager 114  
SECaaS 59  
Secure onboarding and terminations 49  
Security awareness program 74  
Security Log 43  
Security notes 87  
Security Spotlight News 87  
Security standards 77  
Shadow IT 16  
Side effects 88  
SOC 1 70  
SOC2 70  
SOC 3 70  
SOX 19  
SQL Injection 63  
S\_RFC 46  
S\_RFCACL 47  
S\_RFC\_ADM 46  
S-RFCRAIAR 47  
S\_RFC\_SHLP 47  
S\_RFC\_TT 47  
S\_RFC\_TTAC 47  
Standards 17, 73  
Sub-controls 21  
System Log 43  
System, Service, and Communications users 68

## T

Task-based 69  
Testing Procedures 79  
Test scripts 119  
Threat actor 16  
Threat actors 108  
Threat Actors 61  
Trusted RFC 95

**U**

Unmanaged risk 107  
User access review 50  
User Access Reviews 69  
User buffer 101  
User Interface Logging 71, 114  
User Interface redress attack 93  
USOBT 45  
USOBT\_C 45

**V**

Vendor masters 107  
Virtualization 107  
Virtual machine 61  
Vulnerability scoring decision matrix  
90  
Vulnerability Type 88

**X**

XSS 62

**Z**

Zero Day vulnerabilities 95