

American Water Works Association
Dedicated to the World's Most Important Resource™

Utility Risk and Resilience Certificate Program:



Course 2 - Security Practices for Operation and Management

1

Course Purpose

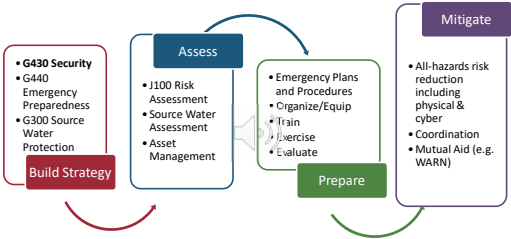
Course 2: Security Practices for Operation and Management

- Demonstrates how to integrate security and preparedness at a utility
- Defines elements of a risk and resilience management strategy, based on G430 standard
- Provides examples of best practices for risk and resilience
- Facilitates compliance with America's Water Infrastructure Act of 2018 (AWIA)

2

Utility Risk & Resilience

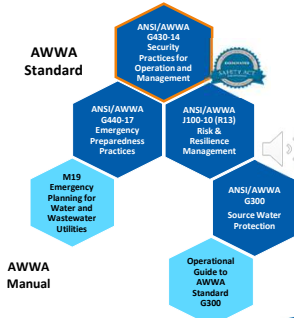


3

Agenda

Elements of a Risk and Resilience Management Strategy:

- Sections 4.1 to 4.5 of G430, including security culture and roles
- Sections 4.6 to 4.9 of G430, including intrusion detection and information protection
- Sections 4.10 to 4.13 of G430, including emergency plans and communication and Sections 5.1 to 5.3 on verification



4

G430 Security Practices Standard


- ANSI/AWWA G430: Security Practices
- Voluntary standard provides minimum recommendations
- Does not supersede regulation or codes
- Is the consensus of the water sector
- Sets the framework for due diligence.

5

Course Handout


- Checklist of G430 elements
- 13 major sections
- 49 documentation points

INSERT LINK TO HANDOUT



6

W74



American Water Works Association
Dedicated to the World's Most Important Resource™

Module 1: Sections 4.1-4.5 of the G430 Standard

7

Learning Objectives

- ✓ Describe how to establish commitment to utility security, build security culture, and define employee roles
- ✓ Explain how security protocols help support AWIA compliance
- ✓ Recognize role of Risk & Resilience Assessment in defining utility priorities.

8

ANSI/AWWA G430: 13 Elements of a Risk & Resilience Management Strategy Module 1

4.1 Explicit Commitment to Security
4.2 Security Culture
4.3 Defined Security Roles and Employee Expectations
4.4 Up-To-Date Assessment of Risk
4.5 Resources Dedicated to Security and Security Implementation Priorities

9

ANSI/AWWA G430: 13 Elements of a Risk & Resilience Management Strategy Module 2

4.6 Access Control and Intrusion Detection
4.7 Contamination Detection, Monitoring and Surveillance
4.8 Information Protection and Continuity
4.9 Design and Construction

10

W60

ANSI/AWWA G430: 13 Elements of a Risk & Resilience Management Strategy Module 3

4.10 Threat Level-Based Protocols
4.11 Emergency Response and Recovery Plans and Business Continuity Plan
4.12 Internal and External Communications
4.13 Partnerships

11

4.1 Explicit Commitment to Security

- Senior Leadership
- Written security plans, policies & procedures
- Visible
- Schedule for updates




G430-14
Section
4.1

12

4.1 Utility Commitment to Security – Examples

- Continuity Plan Umbrella Document
- Utility-wide Committee
- Schedule document updates
- Security Policy
- Key Control Policy



G430-14
Section
4.1

13

13

4.1 How Explicit Commitment to Security Supports AWIA

- Supports the assessment and implementation of security-related mitigation measures
- Supports long-term AWIA compliance
- Supports utility operation and maintenance for resilience



G430-14
Section
4.1

14

14

4.2 Build a Security Culture

- Security is everyone's business!
 - New employee orientation
 - Staff meeting item
 - Newsletter articles
 - Add to existing trainings
 - Hiring, promotions, review
 - Background checks
- Public outreach campaigns
 - Protect water & public health
 - Social media



G430-14
Section
4.2

15

15

4.2 Utility Security Culture – Examples

- Every delivery driver is accompanied by utility staff while on-site
- When operator leaves password on a sticky note at their computer, supervisor reinforces the policy
- Utility Manager says, "Every one of our employees is part of the security staff"



G430-14
Section
4.2

16

16

4.2 How Building a Utility Security Culture Supports AWIA

- Supports long-term AWIA compliance
- Creates the opportunity for continuous improvement of security
- Supports utility operation and maintenance for resilience

G430-14
Section
4.2

17

17

4.3 Define Security Roles and Employee Expectations



Ask law enforcement for free posters, videos, and training



G430-14
Section
4.3

18

18

4.3 Define Security Roles and Employee Expectations

- Security Badges
 - Employees
 - Contractors
 - Visitors
 - Temporary
- Best Practices
 - Badge policy
 - Recent color photo
 - Expiration date
 - Security watermark, hologram






G430-14 Section 4.3 19

19

4.3 Define Security Roles and Employee Expectations

- Identify staff responsible for security
 - Plans
 - Risk and resilience assessments
 - Leadership
 - Program management
 - Intrusion & detection
 - Incident Command
- Establish expectations
- Include in performance evaluations
- Use background checks





G430-14 Section 4.3 20

20

4.3 Utility Security Roles and Employee Expectations - Examples

- Hiring a Security and Emergency Preparedness Manager
 - Consolidated security practices
 - Development of security standard operating procedures
 - Responsibility for updates to plans and better integration of security and resilience functions
 - Shared security responsibility with managers
 - Identified duties in annual reviews




G430-14 Section 4.3 21

21

4.3 How Utility Security Roles and Employee Expectations Supports AWIA

- Setting expectations creates the opportunity for continuous improvement of security-related utility functions
- Supports long-term AWIA compliance
- Supports identification of strategies that can be used to aid in the detection threats and hazards



G430-14 Section 4.3 22


22

Activity

Problem solving scenario:

What free or low-cost actions may help you build and maintain a security culture at your utility?

Select all that apply.



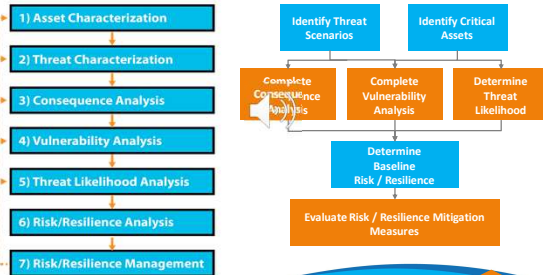
- ☐ Newsletter article
- ☐ Staff meeting agenda item
- ☐ Addition to existing training
- ☐ Leadership proclamation of commitment

G430-14 Section 4.4 23

23

4.4 Risk and Resilience Assessment

Course 3 covers the risk assessment in depth



```

graph TD
    A[1) Asset Characterization] --> B[2) Threat Characterization]
    B --> C[3) Consequence Analysis]
    C --> D[4) Vulnerability Analysis]
    D --> E[5) Threat Likelihood Analysis]
    E --> F[6) Risk/Resilience Analysis]
    F --> G[7) Risk/Resilience Management]
    
    H[Identify Threat Scenarios] --> I[Complete Consequence Analysis]
    J[Identify Critical Assets] --> K[Complete Vulnerability Analysis]
    L[Determine Threat Likelihood] --> M[Determine Baseline Risk / Resilience]
    I --> M
    K --> M
    M --> N[Evaluate Risk / Resilience Mitigation Measures]
  
```

G430-14 Section 4.4 24

24

4.4 Utility Risk and Resilience Assessment Examples

- A utility conducts a risk and resilience assessment:
 - Tests assumptions on the effectiveness of current security practices
 - Identifies low-cost and easily implementable improvements throughout the project

G430-14
Section
4.4

25

25

4.4 How a Risk and Resilience Assessment Supports AWIA

- A Risk and Resilience Assessment (RRA) analyzes:
 - Risks to the system from malevolent acts and natural hazards
 - Resilience of system components
 - Monitoring practices
 - Financial infrastructure of the utility
 - Use, storage, or handling of various chemicals
 - Operation and maintenance
 - Evaluation of capital and operational needs for risk and resilience management for the system
- Sets stage for Emergency Response Plan (ERP) development

G430-14
Section
4.4

26

26

4.5 Dedicated Resources and Priorities



EXERCISES



SECURITY PLAN



IMPROVEMENTS

G430-14
Section
4.5

27

27

4.5 Dedicated Resources and Priorities - Implementing Priorities

- Maintain focus on security
- Maintain security as a priority



G430-14
Section
4.5

28

28

4.5 Utility Dedicated Resources and Priorities – Example: Capital Planning



- All-Hazards projects & prioritization:
 - Short-term/long-term
 - % risk reduction
 - Benefit-cost analysis
 - Capital cost
 - CIP-ready

G430-14
Section
4.5

29

29

4.5 How Dedicated Resources and Priorities Support AWIA

- Dedicated resources demonstrate a commitment to resilience by management
- Dedicated staffing with clear responsibilities
- Dedicated time and effort across the whole organization
- Dedicated capital and O&M funding to address resiliency directly

G430-14
Section
4.5

30

30

W27

Activity

Checklist/self-evaluation:
Which items has your utility already participated in? Check all that apply


- ☐ Leadership commitment
- ☐ Culture of Security
- ☐ Training
- ☐ Exercises
- ☒ J100 RRA
- ☐ Priorities
- ☐ Security improvement plan
- ☐ Budget integration





31

Knowledge Check


Which of the following statements is true?


- A. Utility employees in the field are primarily responsible for maintaining utility commitment to security.
- B. Only designated security staff need to worry about security practices at the utility. 
- C. Customers contribute to maintaining security through raising awareness of possible threats.
- D. Security improvement should be considered secondary to all other utility improvement plans.




32

Module 1 Summary

- 4.1 Explicit Commitment to Security
- 4.2 Security Culture
- 4.3 Defined Security Roles and Employee Expectations 
- 4.4 Up-To-Date Assessment of Risk
- 4.5 Resources Dedicated to Security and Security Implementation Priorities





33



Module 2:


Sections 4.6-4.9 of the G430 Standard

34

Learning Objectives


- ✓ Describe benefits of in-depth defense approach to utility security
- ✓ Explain concepts of deter, detect, devalue, delay, and respond and give examples of each
- ✓ Discuss monitoring system for contamination threats and protecting critical information through cybersecurity
- ✓ Give examples of design and construction projects that prevent intrusions and protect assets.



35

ANSI/AWWA G430: 13 Elements of a Risk & Resilience Management Strategy Module 2

4.6 Access Control and Intrusion Detection
4.7 Contamination Detection, Monitoring and Surveillance
4.8 Information Protection and Continuity
4.9 Design and Construction



36

4.6 Access Control and Intrusion Detection
 4.7 Contamination Detection, Monitoring and Surveillance

G430-14 Section 4.6-4.7

37

4.6 Access Control and Intrusion Detection

Keys

Cards

Bio

G430-14 Section 4.6

38

4.6 Access Control and Intrusion Detection

DETER
 DETECT
 DEVALUE
 DELAY
 RESPOND

G430-14 Section 4.6

39

4.6 Access Control and Intrusion Detection - Explained

Deter
 Detect
 Devalue

- Warning signs
- Lights
- Patrols
- Sensors
- CCTV
- People
- Access Control
- Redundant Pumps
- Backup to Asset

G430-14 Section 4.6

40

4.6 Access Control and Intrusion Detection - Explained

Delay
 Respond

- Barriers
- Hardened Doors
- Fences
- Exercised ERP
- Communications
- Law Enforcement
- Utility Personnel

G430-14 Section 4.6

41

4.6 Access Control and Intrusion Detection

Adversary Task Time

No Security System

With Security System

Alarm Detected

Detect (& Assess)

Delay

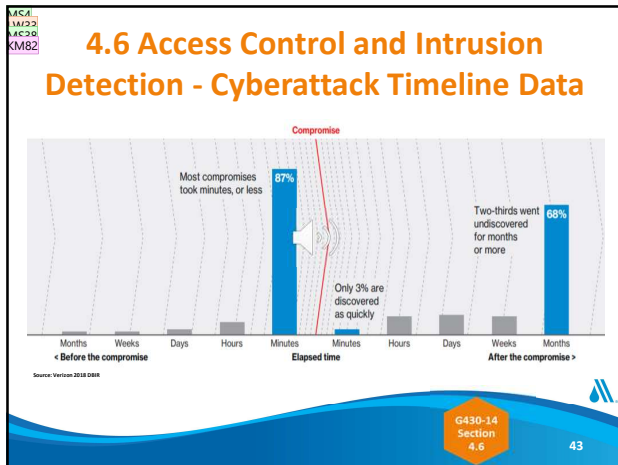
Respond

Adversary Interrupted

Adversary Task Complete

G430-14 Section 4.6

42



43

Activity Slide

Match examples of concepts to pictures:

	Detect		Deter
	Delay		Devalue

G430-14 Section 4.6

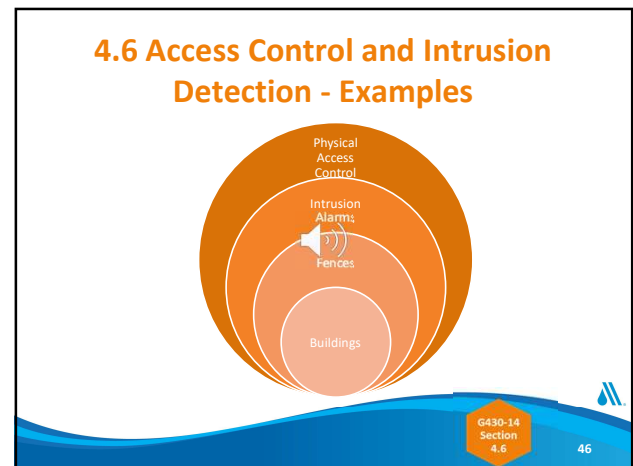
44

4.6 Access Control and Intrusion Detection – Implementing Priorities

- Determine areas requiring access:
 - Critical assets
 - Control systems
 - Chemicals
 - High value areas
 - Plans/drawings
 - HR/Executive offices

G430-14 Section 4.6

45



46

4.6 How Access Control and Intrusion Detection Support AWIA

- Physical barriers: control of access to critical assets
- Means of detecting and assessing intrusion
- Procedures to control personnel access to identified critical assets
- Means of restricting authorization for access

G430-14 Section 4.6

47

4.7 Contamination, Detection, Monitoring and Surveillance

- What is the objective of a contamination warning system?
- What are the appropriate monitoring technologies?
- What do we do when the alarm goes off?

G430-14 Section 4.7

48

4.7 How Contamination, Detection, Monitoring and Surveillance Support AWIA

- Evaluation of source water/intakes, treatment & storage
- Monitoring practices, and threat detection strategies
- Surveillance and response for chemical, biological, or radiological contamination
- Monitoring or surveillance of indicators of contamination.
- Laboratory testing for contaminants
- Communication with customers and public health authorities as a means of identifying contamination
- Incident detection and response plans

G430-14
Section
4.7

49

49

G430 Sections 4.8-4.9

4.8 Information Protection and Continuity

4.9 Design and Construction



G430-14
Section
4.8-4.9

50

50

4.8 Information Protection & Continuity



- ✓ Define
- ✓ Secure
- ✓ Regulations
- ✓ Protection
- ✓ Access



G430-14
Section
4.8

51

51

4.8 Information Protection & Continuity – Example Protecting IT & SCADA



POWER



PHYSICAL &
PROCEDURAL
CONTROLS



DETECT



ENSURE



COMMUNICATIONS



52

52

4.8 How Information Protection & Continuity Support AWIA

- Defines and secures security-sensitive information
- Protects SCADA and other IT systems
- Provides uninterrupted power for IT systems
- Establishes physical procedural controls and detects unauthorized access
- Identifies critical information and communication

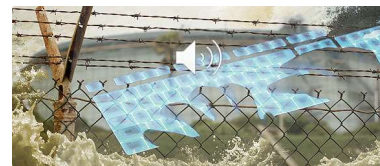


53

53

Where can you learn more about Water Sector Cybersecurity?

<https://www.awwa.org/Cybersecurity>



54

54

4.9 Design & Construction



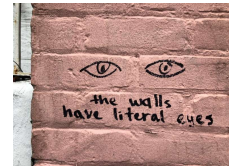
- ✓ Crime Prevention Through Environmental Design (CPTED)
- ✓ Mitigation ideas

55

55

4.9 Design & Construction: CPTED

- Crime Prevention Through Environmental Design (CPTED)
- Examples of strategies to manage risk
 - Concrete flower containers as barriers
 - Murals
 - Human form art on assets
 - Windows on areas
 - Activity in the area



56

56

4.9 Design and Construction: All-Hazards Mitigation Measures



- Apply results
- Multiple benefits
- Iterative process

G430-14
Section
4.9.1.2

57

57

4.9 Utility Design & Construction Examples: CPTED

“The presence of a broken window will entice vandals to break more windows in the vicinity.”
– Wilson and Kelling, 1982 (Atlantic Monthly)



58

58

4.9 Utility Design & Construction Examples: Protection & Mitigation Measures



Flood



Earthquake



Power



Wind



SCADA



Redundancy

G430-14
Section
4.9

59

59

4.9 How Design and Construction Support AWIA

- Incorporates security objectives into utility design and construction standards.
- Physical hardening of identified critical assets.
- Adoption of security risk technologies or approaches.

G430-14
Section
4.9

60

60

Activity Slide

Which one of these strategies is not an example of Crime Prevention Through Environmental Design?

- a. Fake rock covering a valve
- b. Murals
- c. Eyes painted on a storage tank
- d. Windows on areas
- e. Garden hose reel
- f. Activity in the area



61

61

Module 2 Summary

- 4.6 Access Control and Intrusion Detection
- 4.7 Contamination Detection, Monitoring and Surveillance
- 4.8 Information Protection and Continuity
- 4.9 Design and Construction

62

62



Module 3: Sections 4.10-4.13 and 5.1-5.3 of the G430 Standard

63

Learning Objectives

- ✓ Identify networks and resources with whom to communicate and partner to learn of threats and coordinate responses
- ✓ Understand the difference between emergency response plans and business continuity plans
- ✓ Complete verification steps for security program, human resources & equipment verification

64

64

G430 Sections 4.10-4.13

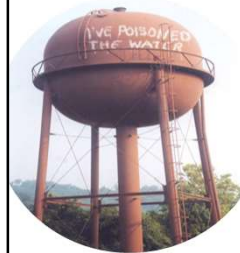
- | |
|---|
| 4.10 Threat Level-Based Protocols |
| 4.11 Emergency Response and Recovery Plans and Business Continuity Plan |
| 4.12 Internal and External Communications |
| 4.13 Partnerships |

G430-14
Section
4.10-4.13

65

65

4.10 Threat Level Protocols



- Monitor DHS advisories
- Additional resources:
 - Local police, fusion center
 - FBI, InfraGard
 - WaterISAC

G430-14
Section
4.10

66

66

Security Threat Intelligence

- DHS
 - <https://www.dhs.gov/protective-security-advisors>
- FBI
 - <https://www.infragard.org/>
- WaterISAC
 - <https://www.waterisac.org/>
- ICS-CERT
 - <https://ics-cert.us-cert.gov/>
- Local law enforcement



67

4.10 Utility Threat Level Protocols - Examples

- Assess credible threats
- Security probes or tests
- Significant crime activity near critical facilities and assets




G430-14 Section 4.10

68

4.10 How Threat Level Protocols Support AWIA

- Monitoring available threat-level information is one type of monitoring practice
- Escalate security procedures in response to relevant threats




G430-14 Section 4.10

69

4.11 Emergency Response Plans and Business Continuity Plans


- ERPs “stop the bleeding” during an emergency
- Business Continuity Plans “keep the heart of the utility” beating during an emergency



G430-14 Section 4.11

70

4.11 Utility Emergency/Continuity Plans - Examples



```


graph TD
    IC[Incident Commander] --> PIO[Public Information Officer]
    IC --> Ops[Operations]
    IC --> Plan[Planning]
    IC --> Log[Logistics]
    IC --> Fin[Finance/Admin]
  
```

G430-14 Section 4.11

71

4.11 Utility Emergency/Continuity Plans - Examples

- Plan updates & reviews
- Mutual aid agreements
- Contact lists
- Response to contamination threat
- Protection of public health



G430-14 Section 4.11

72

4.11 How Emergency/Continuity Plans Support AWIA

- AWIA requires an ERP that must include:
 - Strategies and resources to improve resilience, including physical and cyber security
 - Plans, procedures and equipment to be utilized in response
 - Actions, procedures, equipment to lessen impact on public health
 - Detection strategies

G430-14
Section
4.11

73

73

4.12 Internal and External Communications

- Employees
- Response organizations
- Customers
- Regulatory agencies
- Communications backup systems



G430-14
Section
4.12

74

74

4.12 Utility Internal and External Communications - Examples

- Area utilities worked together to develop a Communications Plan that included:
 - Primary and backup contacts internally and with external agencies
 - Alternate communication technologies
 - Updates to contact information every quarter

G430-14
Section
4.12

75

75

4.12 How Internal and External Communications Support AWIA

- Establishes and maintains strategies for regular and ongoing communications with:
 - Employees
 - Critical Customers
 - Regulatory agencies
 - Emergency Contacts

G430-14
Section
4.12

76

76

4.13 Partnerships

- Identify key agencies and partnerships
- Build collaborative relationships
- Ensure cooperation and effective coordination



G430-14
Section
4.13

77

77

4.13 Utility Partnerships Examples

- Water and Wastewater Agency Response Networks (WARN)
- Emergency Management, Police, Fire (Local Emergency Planning Committee)
- Recovery: Engineering, Transportation, Sanitation
- Local health departments
- Regulatory authorities
- Critical interdependent infrastructure (e.g. power, adjacent utilities)

G430-14
Section
4.13

78

78

4.13 How Partnerships Support AWIA

- Forges reliable and collaborative partnerships with communities served
- Identifies key partnerships essential to emergency response and recovery
- Improves effective coordination during an emergency

G430-14
Section
4.13

79

79

Knowledge Check

Utilities should develop relationships with:

- A) Local, regional, state and federal law enforcement
- B) City/county health department
- C) Regulatory agencies
- D) All of the above

QUIZ

80

G430 Section 5.1 – 5.3

- 5.1 Security Program Verification
- 5.2 Human Resources Verification
- 5.3 Equipment Verification

G430-14
Section
5.1-5.3

81

81

5.1 Security Program Verification

- ✓ Required documentation for a successful risk and resilience management strategy
 - 13 elements
 - 32 documentation points



G430-14
Sec. 5.1 &
Table 1

82

82

5.1 Utility Security Program Verification- Examples

Example Activity: [Click here](#) to review the G430 Handout Checklist

G430-14
Sec. 5.1 &
Table 1

83

83

5.1 How Security Program Verification Supports AWIA

- ✓ Defines Critical Security Activities
- ✓ Documents Security Objectives
- ✓ Documents Security Policy
- ✓ Controls Records

G430-14
Sec. 5.1 &
Table 1

84

84

MS29

5.2 Human Resources Verification



- Competence
- Awareness
- Training

G430-14
Sec. 5.2

85

85

MS29

5.2 Utility Human Resources Verification - Examples

- Job descriptions
- Staff training and performance reviews
- Education
- Hiring and contracting SOPs
- Records Management

G430-14
Sec. 5.2

86

86

5.2 How Human Resources Verification Supports AWIA

- Competent staff on the basis of appropriate education, training, skills, and experience for security and preparedness activities.
- Utilities determine the necessary competence for personnel performing work affecting security and emergency preparedness

G430-14
Sec. 5.2

87

87

MS29
LW106

5.3 Equipment Verification

- Field test security devices (e.g. motion detectors, intrusion sensors) quarterly
- Check passive devices (e.g. fences, gates, doors) every 6 months or as required by law/regulation



G430-14
Sec. 5.3

88

88

5.3 Utility Equipment Verification Examples

- Inspect equipment for:
 - Condition
 - Critical spares and parts
 - Redundancy or contingent bypass operation
 - Adequate protection from SCADA hacking
- Ensure timely replacement

G430-14
Sec. 5.3

89

89

5.3 How Equipment Verification Supports AWIA

- Identification of equipment that can be utilized in the event of a malevolent act or natural hazard
- Identification of actions, procedures, and equipment which can obviate or significantly lessen the impact of a malevolent act or natural hazard

G430-14
Sec. 5.3

90

90

WWS1

Knowledge Check

Which items must a utility protect from public view (and remove from websites) because the information can be used to harm the utility?

- A) Facility Maps
- B) Security Plans
- C) Natural Hazard Mitigation Plans

QUIZ

91

Module 3 Summary

- 4.10 Threat Level-Based Protocols
- 4.11 Emergency Response and Recovery Plans and Business Continuity Plan
- 4.12 Internal and External Communications
- 4.13 Partnerships
- 5.1 Security Program Verification
- 5.2 Human Resources Verification
- 5.3 Equipment Verification

92

American Water Works Association
Dedicated to the World's Most Important Resource™

Course 2 Resources and Summary

93

WWS7

Technical & Programmatic Resources

- AWWA Risk & Resilience:
 - <https://www.awwa.org/Risk> or <https://www.awwa.org/Resilience>
 - <https://www.awwa.org/cybersecurity>
- U.S. EPA:
 - Water Resilience
 - <https://www.epa.gov/waterresilience>
 - Water System Security & Resilience
 - <https://www.epa.gov/homeland-security-research/water-system-security-and-resilience-homeland-security-research>
 - Water Quality Surveillance and Response
 - <https://www.epa.gov/waterqualitysurveillance>

94

WWS8

Steps to a Risk and Resilience Management Strategy

1. Use the G430 standard with J100, G440, and M19
2. Develop a culture of security
3. Use the Risk and Resilience Assessment (RRA) to drive improvements
4. Identify current capabilities
5. Use the RRA to inform emergency response plan strategies and protocols
6. Create a culture of constant improvement

95

G430 Sections Related to AWIA Requirements

Risk & Resilience Assessment Topic from AWIA	G430 Section	Emergency Response Plan Topic from AWIA	G430 Section
- malevolent act	4.4, 4.11	- resilience strategies (physical/cyber)	4.4, 4.10, 4.11
- natural hazards	4.4, 4.11	- plans/procedures for response	4.11, 4.12, 4.13
- pipes /conveyances	4.6		
- source water/intakes	4.6, 4.7		
- treatment & storage	4.6, 4.7, 4.9		
- electronic, computer, automated systems	4.6, 4.8		
- monitoring practices	4.6, 4.7, 4.8		
- financial infrastructure	4.8		
- chemical use, storage, handling	4.6, 4.9		
- operations and maintenance	4.1, 4.2, 4.5, 4.10		
- capital & operational needs	4.5		

96

Course 2 Summary

- Implementation of G430 is a key component of utility risk and resilience management.
- Building upon the risk and resilience assessment to inform the emergency response plan provides mitigation measures for utility resilience.
- Completing the 5 courses in the AWWA Utility Risk and Resilience Certificate Program facilitates development of a utility risk and resilience management strategy.

