ISO 27001:2022 FINAL COUNTDOWN TO TRANSITION

PRESENTED BY: JOHN LAFFEY – ISMS PROGRAM MANAGER FOR PJR

BEFORE WE BEGIN

- ALL PARTICIPANTS HAVE BEEN MUTED FOR CALL CLARITY
- THE SLIDES FROM THIS PRESENTATION WILL BE AVAILABLE SHORTLY FROM WWW.PJR.COM – UNDER 'TRAINING', CLICK 'PAST WEBINAR SLIDES'
  - HTTPS://WWW.PJR.COM/WEBINAR/PAST-WEBINAR-SLIDES
- A RECORDING OF THIS WEBINAR (AND ALL PAST WEBINARS) WILL BE AVAILABLE FOR REVIEW ON YOUTUBE
  - SEARCH 'WWW.YOUTUBE.COM/@PJREGISTRARS' TO VIEW THEM – FREE!

AGENDA

- WHEN IS THE DEADLINE
- WHAT IS THE IMPACT
- MINOR CHANGES TO NUMBERED CLAUSES
- CHANGES TO ANNEX A
- GUIDANCE ON AUDITING NEW CONTROLS
- QUESTIONS & ANSWERS

ISO 27001:2022 TRANSITION DEADLINE

THE OFFICIAL DEADLINE FOR TRANSITIONING TO THE 2022 VERSION OF THE STANDARD IS OCTOBER 31, 2025

- IF YOU ARE CURRENTLY CERTIFIED EXPECT TO TRANSITION PRIOR TO THIS DATE

WHAT IS THE IMPACT

THE OFFICIAL DEADLINE FOR TRANSITIONING TO THE 2022 VERSION OF THE STANDARD IS OCTOBER 31, 2025

- ORGANIZATIONS CURRENTLY CERTIFIED TO THE 2013 VERSION WILL NEED TO TRANSITION BY THE OFFICIAL DEADLINE. AFTER OCTOBER 31ST CERTIFICATIONS TO THE 2013 VERSION WILL NO LONGER BY VALID
- CURRENTLY CERTIFIED ORGANIZATIONS SHOULD PLAN ON TRANSITIONING WELL AHEAD OF TIME AS THE AUDIT NEEDS TO BE CONDUCTED, CORRECTIVE ACTIONS NEED TO BE SUBMITTED AND ACCEPTED, AND PACKAGE REVIEW AND CERTIFICATE ISSUANCE NEED TO BE COMPLETED.
- ALL OF THESE ASPECTS COMPONENTS OF THE CERTIFICATE DECISION TAKE TIME, AND NOT GETTING YOUR AUDIT DONE WELL AHEAD OF THE DEADLINE COULD PUT YOU AT RISK OF HAVING A INVALID CERTIFICATE.
- PJR HAS IMPLEMENTED A DEADLINE FOR ALL OF OUR 2013 CERTIFIED CLIENTS TO TRANSITION NO LATER THAT JULY 31, 2025. THIS IS TO ENSURE THAT THERE IS NO LAPSE IN CERTIFICATION.
- FOR ORGANIZATIONS THAT ARE PLANNING TO BECOME ISO 27001 CERTIFIED, ENSURE YOU ARE USING THE 2022 VERSION OF THE STANDARD FOR YOUR IMPLEMENTATION.

CHANGES TO NUMBERED CLAUSES

CLAUSE 4.2 NOW STATES THAT THE ORGANIZATION SHALL DETERMINE THE RELEVANT REQUIREMENTS OF INTERESTED PARTIES, AND WHICH OF THESE REQUIREMENTS WILL BE ADDRESSED THROUGH THE ISMS.

- THIS MINOR CHANGE NOW SPECIFIES THAT IT IS SPECIFIED WHAT REQUIREMENTS WILL BE ADDRESSED THROUGH THE ISMS
- FOR EXAMPLE AN INTERESTED PARTY MAY HAVE MANY REQUIREMENTS, NOT ALL OF THEM WILL BE RELEVANT TO THE ISMS. THIS CHANGE IS TO ENSURE THAT THE REQUIREMENTS RELATED TO INFORMATION SECURITY ARE IDENTIFIED.

CHANGES TO NUMBERED CLAUSES

CLAUSE 6.2 ADDED SECTION STATING THAT OBJECTIVES BE MONITORED AND THAT THEY BE AVAILABLE AS DOCUMENTED INFORMATION

- THIS CHANGE WAS MADE TO SPECIFICALLY CALL OUT MONITORING OF OBJECTIVES, WHICH WHILE I BELIEVE WAS IMPLIED IN THE 2013 VERSION WAS NOT AN EXPLICIT REQUIREMENT

CHANGES TO NUMBERED CLAUSES

CLAUSE 6.3 IS A NEW CLAUSE THAT STATES THAT WHEN CHANGES NEED TO BE MADE TO THE ISMS THEY SHALL BE CARRIED OUT IN A PLANNED MANNER.

- THIS REQUIREMENT IS LOOKING TO SEE THAT ANY CHANGE MADE TO THE ISMS IS PLANNED AHEAD OF TIME AND DONE IN A ORGANIZED WAY. THIS COULD BE DEMONSTRATED IN A NUMBER OF WAYS INCLUDING RISK ASSESSMENTS BEING PERFORMED PRIOR TO CHANGES, ANY TYPE OF DOCUMENTED PLANNING OR PROJECT MANAGEMENT RELATED TO THE CHANGES ETC.

CHANGES TO ANNEX A

ANNEX A HAS BEEN COMPLETELY REDONE, THE 2022 REVISION CONTAINS 93 CONTROLS RATHER THAN THE 114 THAT WERE IN THE 2013 REVISION.

ANNEX A IS NOW DIVIDED INTO 4 CATEGORIES RATHER THAN THE 14 IN THE 2013 REVISION. THE CATEGORIES ARE AS FOLLOWS:

A.5 – ORGANIZATIONAL (37 CONTROLS)

A.6 – PEOPLE (8 CONTROLS)

A.7 – PHYSICAL (14 CONTROLS)

A.8 – TECHNOLOGICAL (34 CONTROLS)

CHANGES TO ANNEX A

MOST OF THE CONTROLS WILL LOOK FAMILIAR, SOME HAVE BEEN COMBINED INTO A SINGLE CONTROL WHEN THEY WERE MULTIPLE CONTROLS IN THE 2013 REVISION.

THERE ARE, HOWEVER, 11 NEW CONTROLS THAT WE WILL COVER ALONG WITH INFORMATION TO HELP YOU UNDERSTAND THEIR INTENT.

NEW CONTROLS

A.5.7 THREAT INTELLIGENCE

- "INFORMATION RELATING TO INFORMATION SECURITY THREATS SHOULD BE COLLECTED AND ANALYZED TO PRODUCE THREAT INTELLIGENCE."
- DEMONSTRATION OF THIS CONTROLS IMPLEMENTATION CAN INCLUDE EVIDENCE OF RECEIVING THREAT INTELLIGENCE FROM A PROVIDER SUCH AS HARDWARE/SOFTWARE MANUFACTURERS, GOVERNMENT AGENCIES, INFORMATION SECURITY ASSOCIATIONS ETC.
- ADDITIONALLY, BEING ABLE TO DEMONSTRATE THAT THIS INFORMATION IS ACTUALLY BEING LOOKED AT AND ACTED UPON WHEN NECESSARY IS CRUCIAL.
- IS THERE A PROCESS IN PLACE TO COMMUNICATE THIS INFORMATION TO THE PEOPLE WHO CAN USE IT?

NEW CONTROLS

A.5.23 INFORMATION SECURITY FOR THE USE OF CLOUD SERVICES

- "PROCESSES FOR ACQUISITION, USE, MANAGEMENT AND EXIT FROM CLOUD SERVICES SHOULD BE ESTABLISHED IN ACCORDANCE WITH THE ORGANIZATION'S INFORMATION SECURITY REQUIREMENTS."
- HAS A POLICY ON THE USE OF CLOUD SERVICES BEEN DOCUMENTED?
- HAVE SHARED INFORMATION SECURITY RESPONSIBILITIES BETWEEN THE PROVIDER AND ORGANIZATION BEEN DEFINED AND IMPLEMENTED?
- IS THERE EVIDENCE CLOUD SERVICE AGREEMENTS ARE BEING REVIEWED TO ENSURE THAT INFORMATION SECURITY IS BEING ADDRESSED?
- HAS A RISK ASSESSMENT BEEN CONDUCTED IN RELATION TO USING THE CLOUD SERVICE?
- HAS DUE DILIGENCE BEEN CONDUCTED REGARDING THE CLOUD SERVICE PROVIDERS INFORMATION SECURITY CAPABILITIES/COMPLIANCE?

NEW CONTROLS

A.5.30 ICT READINESS FOR BUSINESS CONTINUITY

- "ICT READINESS SHALL BE PLANNED, IMPLEMENTED, MAINTAINED AND TESTED BASED ON BUSINESS CONTINUITY OBJECTIVES AND ICT CONTINUITY REQUIREMENTS"
- HAS A BUSINESS IMPACT ANALYSIS (BIA) BEEN CONDUCTED, OR HAS A BUSINESS CONTINUITY PLAN (BCP) BEEN DOCUMENTED?
- HAVE CRITICAL SERVICES/ACTIVITIES BEEN IDENTIFIED? HAS A RECOVERY TIME OBJECTIVE (RTO) BEEN ASSIGNED TO THE PRIORITIZED SERVICES?
- ARE PLANS BEING REGULARLY TESTED?
- DO THE PLANS INCLUDE PROCEDURES FOR RESTORING THE ICT SERVICES?

NEW CONTROLS

A.7.4 PHYSICAL SECURITY MONITORING

- "PREMISES SHALL BE CONTINUOUSLY MONITORED FOR UNAUTHORIZED PHYSICAL ACCESS"
- THIS CONTROL IS LOOKING TO SEE THAT PHYSICAL PREMISES ARE BEING MONITORED IN SOME FASHION. IT DOES NOT REQUIRE ANY 1 SPECIFIC TYPE OF MONITORING. COMMON EXAMPLES SEEN INCLUDE VIDEO MONITORING SYSTEMS, MOTION DETECTORS, ALARM SYSTEMS, CONTACT DETECTORS, GUARDS/FRONT DESK PERSONNEL WHO VERIFY VISITORS IDENTIES AND CONFIRM THEY ARE AUTHORIZED TO ENTER ETC.

NEW CONTROLS

A.8.9 CONFIGURATION MANAGEMENT

- "CONFIGURATIONS, INCLUDING SECURITY CONFIGURATIONS, OF HARDWARE, SOFTWARE, SERVICES AND NETWORKS SHALL BE ESTABLISHED, DOCUMENTED, IMPLEMENTED, MONITORED AND REVIEWED"
- HAVE ROLES AND RESPONSIBILITIES BEEN ASSIGNED IN REGARD TO CONFIGURATION CHANGES?
- IS A PROCEDURE IN PLACE FOR CONFIGURATION CHANGES?
- IS A STANDARD TEMPLATE OR IMAGE USED FOR CONFIGURING HARDWARE?
- ARE CONFIGURATIONS MANAGED FOLLOWING THE CHANGE MANAGEMENT PROCESS?
- ARE CONFIGURATIONS BEING MONITORED AND UPDATED WHEN NECESSARY?

NEW CONTROLS

A.8.10 INFORMATION DELETION

- "INFORMATION STORED IN INFORMATION SYSTEMS, DEVICES OR IN ANY OTHER STORAGE MEDIA SHALL BE DELETED WHEN NO LONGER REQUIRED"
- DOES THE ORGANIZATION HAVE A DATA RETENTION POLICY?
- HAVE METHODS OF DELETION BEEN SPECIFIED?
- IF A THIRD PARTY STORES THE ORGANIZATIONS INFORMATION ON ITS BEHALF, IS THERE AN AGREEMENT THAT THE INFORMATION WILL BE DELETED UPON TERMINATION OF THE SERVICE?
- IF A SECURE DISPOSAL SERVICE PROVIDER IS BEING USED ARE THEY APPROVED? HAVE THEY BEEN VETTED FOR INFORMATION SECURITY CAPABILITIES?

NEW CONTROLS

A.8.11 DATA MASKING

- "DATA MASKING SHALL BE USED IN ACCORDANCE WITH THE ORGANIZATION'S TOPIC-SPECIFIC POLICY ON ACCESS CONTROL AND OTHER RELATED TOPIC-SPECIFIC POLICIES, AND BUSINESS REQUIREMENTS, TAKING APPLICABLE LEGISLATION INTO CONSIDERATION"
- DOES THE ORGANIZATION HANDLE SENSITIVE INFORMATION SUCH AS PII?
- IS ENCRYPTION BEING USED WHEN AND WHERE NECESSARY?
- IS THE ORGANIZATION USING PSEUDONYMIZATION OR ANONYMIZATION TECHNIQUES?

NEW CONTROLS

A.8.12 DATA LEAKAGE PREVENTION

- "DATA LEAKAGE PREVENTION MEASURES SHOULD BE APPLIED TO SYSTEMS, NETWORKS AND ANY OTHER DEVICES THAT PROCESS, STORE OR TRANSMIT SENSITIVE INFORMATION"
- HAS THE ORGANIZATION IDENTIFIED AND CLASSIFIED INFORMATION THAT NEEDS TO BE PROTECTED AGAINST LEAKAGE?
- IS THERE ANY TYPE OF MONITORING OF CHANNELS OF DATA LEAKAGE SUCH AS EMAIL, FILE TRANSFERS, MOBILE DEVICES, PORTABLE STORAGE DEVICES?
- IF A DATA LEAKAGE PREVENTION TOOL IS BEING USED, IS IT IDENTIFYING AND MONITORING SENSITIVE INFORMATION AT RISK?
- IS THE TOOL DETECTING DISCLOSURE OF SENSITIVE INFORMATION?
- IS IT BLOCKING USER ACTIONS THAT EXPOSE SENSITIVE INFORMATION (EMAILING SENSITIVE INFORMATION, EXPORTING A DATABASE TO A SPREADSHEET)?
- THIS CONTROL DOES NOT REQUIRE THE USE OF A DLP TOOL OR SOLUTION, AS THEY ARE TYPICALLY VERY EXPENSIVE, BUT ONE MAY BE PRACTICAL FOR AN ORGANIZATION THAT HANDLES HIGHLY SENSITIVE DATA.

NEW CONTROLS

A.8.16 MONITORING ACTIVITIES

- "NETWORKS, SYSTEMS AND APPLICATIONS SHOULD BE MONITORED FOR ANOMALOUS BEHAVIOR AND APPROPRIATE ACTIONS TAKEN TO EVALUATE POTENTIAL INFORMATION SECURITY INCIDENTS"
- DOES THE ORGANIZATION HAVE ANY TYPE OF MONITORING IN PLACE?
- DOES THE MONITORING PROVIDE ALERTS IF SPECIFIED THRESHOLDS OR EVENTS OCCUR?
- ARE THEY MONITORING LOGS, NETWORK ACTIVITY, UTILIZATION OF RESOURCES (BANDWIDTH, STORAGE, CPU, MEMORY)?
- IS THE MONITORING BEING USED TO TAKE ACTION TO AVOID OR MINIMIZE ADVERSE AFFECTS?
- THIS CONTROL DOES NOT REQUIRE THE USAGE OF A SIEM.

NEW CONTROLS

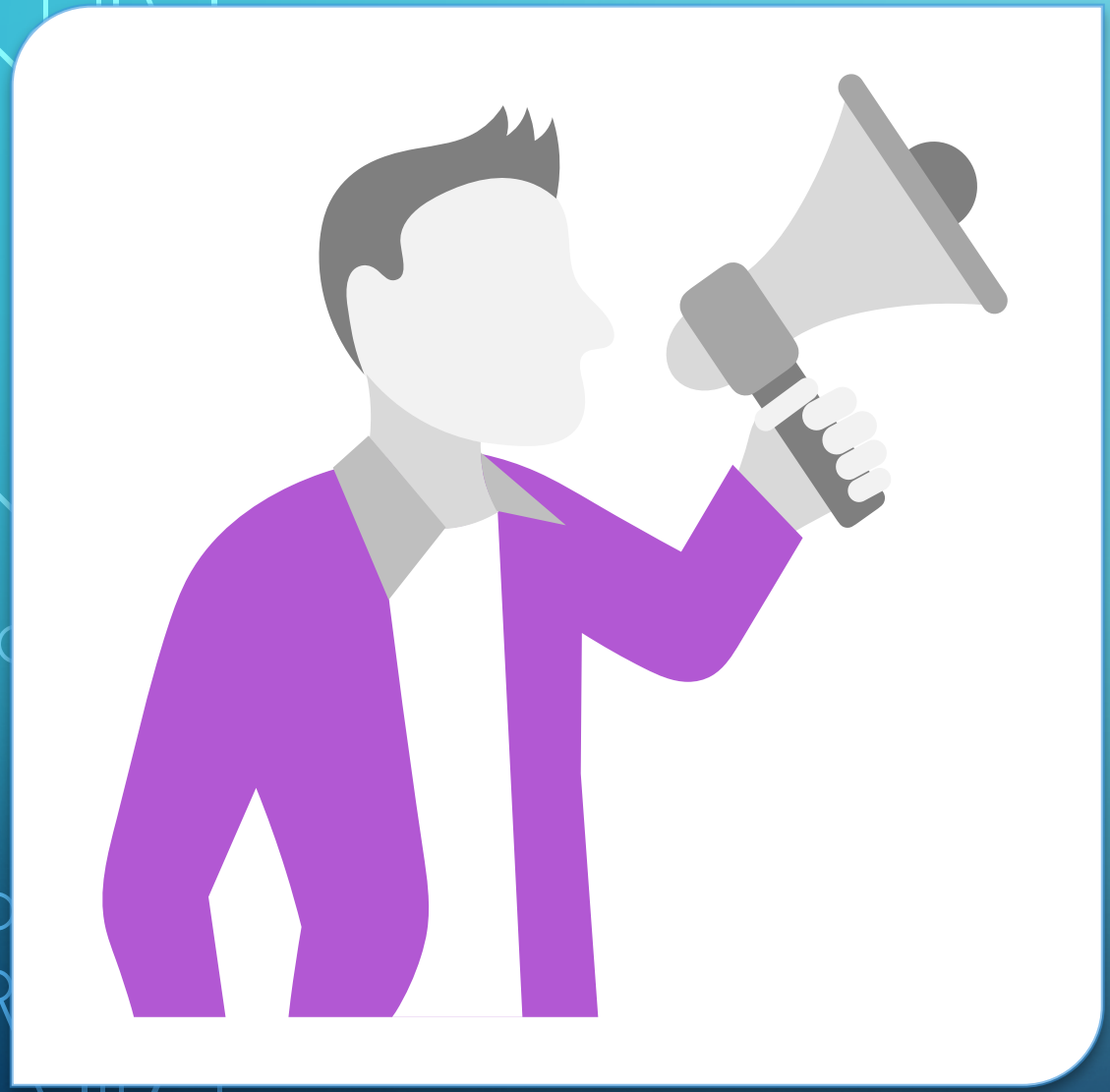
A.8.23 WEB FILTERING

- "ACCESS TO EXTERNAL WEBSITES SHALL BE MANAGED TO REDUCE EXPOSURE TO MALICIOUS CONTENT"
- IS THERE ANY TOOL IN PLACE THAT PREVENTS USERS FROM ACCESSING WEBSITES THAT CONTAIN MALICIOUS CONTENT (BROWSER BASED, ANTIVIRUS, FIREWALL CONFIGURATIONS ETC.)?
- HAS THE ORGANIZATION DOCUMENTED SAFE AND APPROPRIATE USE OF ONLINE RESOURCES, INCLUDING RESTRICTIONS TO UNDESIRABLE OR INAPPROPRIATE WEBSITES?
- HAVE USERS BEEN TRAINED ON THE SECURE AND APPROPRIATE USE OF ONLINE RESOURCES?

NEW CONTROLS

A.8.28 SECURE CODING

- "SECURE CODING PRINCIPLES SHOULD BE APPLIED TO SOFTWARE DEVELOPMENT"
- HAVE PROCESSES BEEN ESTABLISHED TO PROVIDE GOVERNANCE FOR SECURE CODING?
- DOES THE GOVERNANCE ALSO COVER SOFTWARE COMPONENTS FROM THIRD PARTIES AND OPEN SOURCE SOFTWARE?
- ARE SECURE CODING PRINCIPLES BEING USED IN THE PLANNING, CODING, AND MAINTENANCE STAGES OF THE SOFTWARE DEVELOPMENT LIFECYCLE?
- IS THERE EVIDENCE THAT SECURITY TESTING IS BEING CONDUCTED DURING AND AFTER DEVELOPMENT?



QUESTIONS & ANSWERS

CONTACT US AT 1-800-800-7910 FOR FURTHER INFORMATION REGARDING 27001 CERTIFICATION

REACH OUT TO ME AT JLAFFEY@PJR.COM WITH ANY FURTHER QUESTIONS OR COMMENTS

THANK YOU FOR ATTENDING!

DOWNLOAD THESE SLIDES AT
WWW.PJR.COM

VIEW A RECORDING OF THIS PRESENTATION ON YOUTUBE ON OUR CHANNEL – PERRY JOHNSON REGISTRARS