Cyber Resilience Readiness Certification

Review Process Guide

March 2026

Issue Date: March 1, 2026

Contents

Part I: Review Preparations **3**

General Guidance and Overview *4*

Part II: Agenda-Specific Activities **6**

Opening Conference *7*

Planning Session and Program Document Review *8*

Clinical Continuity Tracer Activity *9*

CRR Annual Exercises and Performance Improvement *11*

Summary Discussion *14*

Reviewer Report Preparation *15*

Exit Conference *16*

Appendix A: Clinical Tracer Scenarios **17**

Appendix B: Evidence of Standards Compliance **25**

General Guidance and Overview

The purpose of the ***Review Process Guide (RPG)*** is to inform organizations and reviewer about the Cyber Resilience Readiness (CRR) review process.

Organizations are encouraged to do the following documents prior to their review:

- Download and review the agenda (as applicable to their program) from Joint Commission's website. If hyperlink does not work, copy and paste https://www.jointcommission.org/jc-connect/review-agenda into your web browser.
- Review CRR chapter requirements listed in the ***Comprehensive Certification Manual for Cyber Resilience Readiness*** on your organization's E-dition..
- Read ***Joint Commission News*** each month for any updates of new and/or revised CRR requirements. *JC News* is posted monthly to your organization's *Joint Commission Connect*® extranet site or can be found on Joint Commission's website in the Knowledge Library.

Prereview Outreach
A Joint Commission account executive will contact your organization by phone or e-mail shortly after receiving the application for certification or recertification. The purpose of this call or e-mail is to:

- Confirm information reported in the application for certification or recertification.
- Verify travel planning information and directions to office(s) and facilities.
- Confirm access to *Joint Commission Connect* and the certification-related information available there.
- Confirm accuracy of any program-specific eligibility requirements, such as completion of the self-assessment.
- Answer any organization-related questions and address any concerns.

Logistics Planning

The account executive will confirm the following with your organization:

- The reviewer will need workspace for the duration of the visit. A desk or table and access to an electrical outlet and the Internet are desirable.
- Some review activities will require a room or area that will accommodate a group of participants. Group activity participants should be limited, if possible, to key individuals who can provide insight into the topic of discussion. Participant selection is left to the organization's discretion; however, this guide does offer suggestions.

- The reviewer will want to move throughout the facility or offices during tracer activity, talking with staff when conducting clinical tracers. The reviewer will rely on organization staff to find locations where discussions can take place that allow confidentiality and privacy to be maintained and that will minimize disruption to the area being visited.

NOTE: *For all reviews, electronic recordings, including artificial intelligence or other transcribing platforms, are **not** allowed per Joint Commission policy.*

Information Evaluated Prior to Certification Review

The assigned reviewer will assess the following information prior to the certification review:

1. Demographic information
2. Self-assessment information
3. Consultation/education provided

Your organization will upload program-specific documents according to the current document list located on *Joint Commission Connect*. Document upload must be completed by the due date listed in the "What's Due" section. Your account executive can assist with the process in advance of certification review, if needed.

Questions About Standards

To submit a question:

- Log in to *Joint Commission Connect* and click on Resources - Standards Interpretation.

  OR
- If the individual submitting a question does not have access to *Joint Commission Connect,* they can do so on Joint Commission's Standards Interpretation Page.

Please contact your Joint Commission account executive with questions about the review process, agenda, scheduling, and so on.

Opening Conference

Objective
To gain a better understanding of the organization's cybersecurity and clinical continuity readiness and response program, as well as answer any questions.

Organization Participants
- Program administrative and clinical leaders, individual(s) who will provide the Safety Briefing to the reviewer, and others at the discretion of the organization.

Materials Needed
- Prepared presentation
  Note: While not required, many organizations choose to prepare a slide deck for providing an introductory overview to the organization and program being evaluated.

What Will Take Place
- The reviewer will begin this session with a few remarks and introduction of themselves, followed by an introduction of the program staff
- The organization is requested to provide the reviewer with a Safety Briefing (informal, no more than five minutes) sometime during this activity. The purpose of this briefing is to inform the reviewer of any current organization safety or security concerns and how Joint Commission staff should respond if the safety plans are implemented while they are on site. Situations to cover include:
  - Fire, smoke, or other emergencies
  - Workplace violence events (including active shooter scenarios)
  - Any contemporary issues the reviewer may experience during the time they are with the organization (for example, seasonal weather-related events, anticipated or current civil unrest, labor action)
- Next, hospital and/or program leaders will present an overview (prepared presentation) of their cybersecurity and clinical continuity readiness and response program. Organizations determine the best format to present the overview of their cybersecurity journey and lessons learned.
- The reviewer will end the session with:
  - Overview of agenda and objectives
  - Dialogue about what the reviewer can do to help make this a meaningful review for the program

Planning Session and Program Document Review

Objective
During this session, the reviewer will go through the documents the hospital needs to have available and in conjunction with CRR program representatives and will identify the departments/services and patients to trace related to clinical continuity processes.

Organization Participants
- Program representative(s) who will facilitate this activity

Materials Needed

- Committee activity documentation (such as meeting minutes and attendance records) for at least the past year
- Annual exercises and six-month exercises if actual substantial incident occurred in the past three years
- Any findings, after-action reports, action plans, improvement plans, and reports identifying changes and updates to the cybersecurity clinical continuity program because of annual exercises or an actual incident

THERE IS NO NEED TO PRINT DOCUMENTS FOR THE REVIEW DAY. To support sustainability efforts, electronic access through screen sharing is preferred.

Clinical Continuity Tracer Activity

Objectives

To learn about the preparedness and response processes for units/departments that will be implemented to maintain continuity of care in the event of a significant cybersecurity incident

Organization Participants

- Individual(s) responsible for coordinating clinical continuity during cyber events in the selected areas
- Unit/department staff

What Will Take Place

The reviewer will select areas to trace and will complete approximately five individual tracer activities. The following topics will be discussed with the selected department/unit staff in greater depth:

  - Manual policies/procedures/processes
  - How staff are informed of activation of manual processes
  - Availability of additional staff to support manual processes
  - Coordination of response efforts with other departments
  - Processes to recover and return to usual activities

- Organization/program staff and the reviewer will move through the selected areas, as appropriate, visiting and speaking with staff in all the areas selected for these tracers.
- Staff will walk the reviewer through the established manual processes for providing care to selected patients.
  NOTE: *The number of staff participating in the tracer activity should be limited. The rationale for limiting the number of staff participating is to reduce any distraction that the review process may have on patient care.*

- Throughout tracer activity, the reviewer will:

  - Observe program staff and patient interaction
  - Observe the care planning process
  - Observe medication processes, if applicable
  - Consider the impact of the environment on individual safety and staff roles in minimizing environmental risk
  - Speak with staff about the care, treatment, and services they provide

    - Look at procedures or other documents, as needed, to verify processes or to further answer questions that still exist after staff discussions

- Throughout the tracer activity, the reviewer will communicate with the program leaders and care providers any:
    - Specific observations made
    - Issues that will continue to be explored in other tracer activity
    - Need for additional record review
    - Issues that have the potential to result in Requirements for Improvement
    - Staff files needed for the Competency Session

See Appendix A for a list of potential tracer scenarios that will be selected for this activity.

Conclusion

- Summarize strengths and potential risk points.
- Transition to the next activity.

CRR Annual Exercises and Performance Improvement

Objectives

To learn about the following:

- Plans for annual testing of clinical continuity preparedness
- Annual tests and improvements or changes made as a result
- Actual incident(s) and response to the incident(s)
- Changes the organization has made to improve its preparedness and response for substantial cybersecurity incidents

Organization Participants

- Program administrative and clinical leaders
- Others at the discretion of the organization

Materials Needed

- Supporting documentation of actions taken, such as updates to policies and procedures, plans, processes

What Will Take Place

The following topics will be discussed in greater depth:

- Lessons learned and experiences the organization wants to share if there was an actual substantial cybersecurity incident (if the organization is comfortable with the discussion) that occurred in the past 12/24/36 months. Topics to discuss in detail include:
    - Impact on organization departments
    - Staff performance of responsibilities
    - Communication to staff related to the event, including updates
    - Communication with relevant authorities and other health care organizations
    - Impact on patient care
    - Coordination of response efforts

- Lessons learned and experiences related to one or two of the organization's annual exercises from the past 12/24/36 months. Topics to discuss in detail include:
    - How or why the exercise(s) was selected
    - How the exercise(s) stressed (fully tested) the clinical continuity response procedures
    - Which staff and departments were involved
    - How were staff involved

- Findings of the organization’s exercises and any actual events during the past three years. Topics to discuss in detail include:
    - What went well
    - What did not go well
    - What changes were made
    - How changes were tested to determine improvement
    - What actions were taken if the changes did not result in improvement

Competency Session

Objective
To discuss and verify how the program meets the need for qualified and competent staff for its CRR program

Organization Participants
- Individuals responsible for program education

What Will Take Place
- Orientation and training process for cybersecurity that is applicable to the roles and responsibilities of staff and/or providers
- Methods for assessing competence of practitioners and team members
- Inservice and other education and training activities
- Review of at least one file per discipline of those staff involved in the program
- Review of cyber resilience readiness education and training plan
- Review of staff files selected during tracer activity to verify staff cyber resilience readiness education and training

Summary Discussion

Objective
To provide time for a final discussion prior to the reviewer's report preparation and the Exit Conference

Organization Participants
- Program leaders
- Others at the discretion of the program

Materials Needed
- Will vary depending upon the review

Topics
- Any issues not yet resolved (IOUs)
- Identified Requirements for Improvement (RFIs)
- What made the review meaningful to the team
- Best practices to inspire quality improvement and/or outcomes
- Educational activities of value to the program (for example, sharing knowledge related to clinical practice guidelines or the latest scientific breakthroughs)
- Whether the goals of the team were met

Reviewer Report Preparation

Objective
To compile, analyze, and organize the data collected into a summary report of observations made throughout the review

Organization Participants
- None required, unless specifically requested by the reviewer

Materials Needed
- None; private workspace for the reviewer with access to an electrical outlet and Internet connection, if available

What Will Take Place
The reviewer uses this time to enter their observations that reflect standards compliance issues. If organization interruptions can be kept to a minimum during this time, it will help the reviewer remain on schedule and deliver a report at the appointed time. The reviewer will be using their tablet to prepare the Preliminary Certification Report and plan for the Exit Conference.

Exit Conference

Objective
To provide the organization with a Preliminary Certification Report of findings from the reviewer

In addition to the preliminary report, the reviewer will:
- Review the Preliminary Certification Report, including the *Survey Analysis for Evaluating Risk*® (*SAFER*®) Matrix.
- Discuss any standards compliance issues that resulted in RFIs.
- Allow the organization a final on-site opportunity to question the review findings and provide additional material regarding standards compliance.
- Explain the post-review clarification process.
- Review required follow-up actions, as applicable.

Organization Participants
- Program leaders
- Clinical leaders
- Other staff at the discretion of the organization

Materials Needed
- None required

What Will Take Place

During the Exit Conference or at the close of day, the reviewer will post the Preliminary Certification Report to the organization's *Joint Commission Connect*® extranet site.

The Final Certification Report and certification decision is made by Joint Commission's Central Office within 10 days of the review and will be posted on *Joint Commission Connect*.

Clinical Tracer Scenarios

The following scenarios may be selected for the CRR review. The questions listed for each scenario are not intended to be a comprehensive list of topics but may be used when conducting tracers.

Infant Abduction Prevention

Security Measures

- How are doors and access points manually secured during outages?
- How is staff assigned to monitor entrances/exits?
- How is restricted access communicated?
- How are infants kept safe within rooms (for example, bassinet placement, transport escorting)?
- How is CCTV functionality maintained and verified without the network?
- How are areas without camera coverage monitored?
- How do security and nursing staff coordinate manual surveillance and response?

Procedural Safeguards

- How are infant transfers manually documented?
- How are staff IDs and credentials verified manually?
- How are authorized personnel lists maintained?
- How are visitors signed in, verified, and escorted?
- How are infant/parent ID bands verified and documented manually?

Documentation

- How will you reconcile manual records with electronic systems once restored?

Communication

- What manual communication tree is used (Code Pink, alerts, updates)?
- What backup communication methods are used (radios, landlines, runners)?
- How are contact lists maintained?
- How is manual communication documented?
- How are internal staff and external agencies notified during an event?

Training and Drills

- How often are outage-related drills conducted?
- How are manual infant-tracking and response processes practiced?
- How are drills debriefed and protocols updated?
- How are protocols and policies and procedures kept current?
- How are new staff trained on outage procedures?

Laboratory

Procedural Safeguards

- **Specimens**
  - What is the process for specimen collection?
  - What is the process for labeling specimens and making sure the correct tests are performed on the specimens?
  - How will staff have access to diagnosis-based order sets and decision supports associated with them (for example, hepatitis panel)?
  - How will you track specimens and prevent loss/delay?
- **Equipment**
  - How will lab equipment be used if it needs to be off network?
- **Test Results**
  - How will you provide timely test results to the correct care providers, including critical test results?
  - How will you provide reports with reference ranges/results?
  - Do you have additional staff to support paper-based processes, such as providing test results to care providers?
- **Documentation**
  - How will you document order information, patient testing information, and results?
  - How will you reconcile manual records with electronic systems once restored?

Communication

- How will you communicate within the laboratory department as well as with other departments/units, such as the emergency department, med/surg, ICU, and pharmacy?
- How will you be notified of testing requests?
  - How will you be notified when tests are needed stat?
- How will you communicate laboratory testing results with care providers?
- How will you coordinate tests performed by outside laboratories (for example, transporting specimens, obtaining results)?

Training and Drills

- How often are outage-related drills conducted?
- How are manual processes practiced?
- How are drills debriefed and protocols updated?
- How are protocols and contact lists kept current?
- How are new staff trained on outage procedures?

Pharmacy

Procedural Safeguards

- **Medication Ordering and Documentation**
  - How are medication orders entered manually during downtime?
  - What paper medication administration records are used to track administered doses?
  - How are manual logs maintained for all dispensed medications, including controlled substances?

    - How is two-person verification ensured for high-risk medications?
- **Inventory Management**
    - How is inventory tracked manually during outages?
    - Can automated dispensing cabinets (ADCs) operate independently or on generator power during outages?
    - What is the manual process for filling and labeling medications if ADCs are down?
- **Staffing and Workflow Adjustments**
    - How is extra staffing assigned to support manual workflows?
    - What shift rotation strategies are used to prevent staff burnout?
    - Who serves as the safety officer or downtime coach for pharmacy operations?
- **Controlled Substances and Compliance**
    - How are paper logs used to track controlled substances?
    - How are manual records reconciled with electronic systems once restored?
- **Refrigerated and Specialty Medications**
    - How are refrigeration and storage conditions monitored manually?
    - What is the procedure when temperature integrity is compromised?
    - How are room-temperature stability rules (for example, 28-day rule) applied during outages?

Communication

- What communication methods are used (landlines, fax, radios, runners)?
- What manual communication method is used for urgent updates?
- How are STAT orders and critical needs communicated manually to care teams?

Training and Drills

- How often are outage-related drills conducted?
- How are manual processes practiced?
- How are drills debriefed and protocols updated?
- How are protocols and contact lists kept current?
- How are new staff trained on outage procedures?
- How are manual records reconciled with electronic systems once restored?

Emergency Department

Procedural Safeguards

- **Patient Registration and Tracking**
    - How does the emergency department (ED) record patient demographics and arrival times using paper forms?
    - How are manual tracking numbers assigned to patients?
    - How does the ED maintain manual triage and room assignment logs?
- **Clinical Documentation**
    - What downtime forms are used for assessments, orders, and progress notes?
    - How are STAT orders prioritized?

    - How is dictation used for provider notes during downtime?
    - How are manual records reconciled with electronic systems once restored?
- **Medication and Orders**
    - How are hard-copy medication orders completed and processed?
    - How are manual medication administration records used to track medication administration?
    - How does the ED coordinate with pharmacy using nonelectronic communication?
- **Lab and Imaging Coordination**
    - How are manual requisition forms used for lab and imaging orders?
    - How are specimens and imaging requests tracked on paper?
    - How are test and imaging results communicated manually?
- **Patient Monitoring and Safety**
    - What non-networked monitoring equipment is used during outages?
    - How is staff rounding frequency adjusted when alerts are unavailable?
    - How are critical patients visually monitored without electronic systems?
- **Staffing and Workflow Adjustments**
    - Who serves as the ED safety officer or downtime coach?
    - How are staff rotations adjusted to prevent fatigue during extended outages?

Communication

- What manual communication tree is used for alerts and coordination?
- What redundant communication systems (landlines, radios, runners) are used?
- How are printed contact lists maintained and accessed?

Training and Drills

- How often are outage-related drills conducted?
- How are manual processes practiced?
- How are drills debriefed and protocols updated?
- How are protocols and contact lists kept current?
- How are new staff trained on outage procedures?
- How are manual records reconciled with electronic systems once restored?

Radiology

Procedural Safeguards

- **Operational Continuity Procedures**
    - How does the department activate downtime protocols?
    - How are scheduling and documentation completed using printed forms or downtime kits?
    - How are paper requisitions used for imaging orders?
    - How is a manual log of completed studies maintained?

    - How does the department ensure that backup picture archiving and communication system (PACS) or offline radiology information system (RIS) access is functional?
- **Prioritization of Imaging**
    - How are imaging requests triaged based on clinical urgency?
    - How does Radiology confirm critical needs with referring departments?
    - How are nonurgent studies deferred until systems are restored?
- **Equipment Functionality**
    - How is imaging equipment operated independently from network systems?
    - How are images stored locally when PACS is unavailable?
    - How are images labeled and stored for later upload and reconciliation?
- **Roles and Responsibilities**
    - **Radiology Technologists**
        - How do technologists perform imaging using manual workflows?
        - How do technologists record patient and study details on paper forms?
        - How do technologists ensure accurate image labeling and storage?
    - **Radiologists**
        - How do radiologists provide verbal or handwritten preliminary reports?
        - How do radiologists coordinate with clinical teams for urgent reads?
        - How are manual findings documented and stored securely?
    - **Radiology IT Support**
        - How are RIS/PACS recovery protocols initiated?
        - How is system status monitored and communicated?
        - How is data reconciliation supported after the outage?
- **Documentation and Data Integrity**
    - What downtime forms are used for patient ID, orders, procedure notes, and preliminary reports?
    - How are paper records reconciled with electronic systems after restoration?
    - How are stored images uploaded to PACS once systems return?
    - How are backlogged data entered into RIS/electronic health records with appropriate timestamps?

Communication

- What nonelectronic communication methods (radios, landlines, messaging apps) are used?
- How are printed contact lists maintained and accessed?
- Who serves as the communication triage lead?
- How are communications documented (such as in a downtime logbook)?

Training and Drills

- How often are outage-related drills conducted?
- How are manual processes practiced?
- How are drills debriefed and protocols updated?

- How are protocols and contact lists kept current?
- How are new staff trained on outage procedures?

Telemedicine Services

Procedural Safeguards

- **Activation of Downtime Protocols**
  - How does the team switch to manual scheduling and documentation during an outage?
  - How are telemedicine staff and clinical partners notified of the outage?
  - How does the organization decide which virtual visits to suspend?
- **Patient Access and Communication**
  - What nonelectronic methods are used to communicate with patients and providers?
  - How are patients provided with alternative contact numbers for urgent needs?
  - How is a printed list of scheduled telemedicine appointments maintained and used for outreach?
- **Clinical Documentation**
  - What downtime documentation forms are used for assessments, orders, and notes?
  - How are manual consent forms obtained and recorded?
  - How are patient interactions and clinical decisions logged for later reconciliation?
- **Provider Coordination**
  - Who serves as the downtime coordinator for provider scheduling and flow?
  - What printed protocols and contact lists support provider coordination?
  - How do providers access manual reference materials when systems are down?
- **Technology and Equipment**
  - What non-networked devices are used to continue telemedicine services during outages?
  - What backup power sources are available for essential telemedicine equipment?
  - How is manually used equipment documented and secured?
- **Privacy and Compliance**
  - What safeguards ensure HIPAA compliance during manual operations?
  - How is the use of personal devices controlled during outages?
  - How are paper records secured and access restricted?

Communication

- What nonelectronic communication methods (radios, landlines, messaging apps) are used?
- How are printed contact lists maintained and accessed?
- Who serves as the communication triage lead?
- How are communications documented (such as in a downtime logbook)?

Training and Drills

- How often are outage-related drills conducted?

- How are manual processes practiced?
- How are drills debriefed and protocols updated?
- How are protocols and contact lists kept current?
- How are new staff trained on outage procedures?

Inpatient Units

Procedural Safeguards

- **Patient Admission and Tracking**
  - How are patient demographics, room assignments, and admission times recorded using paper forms?
  - How are manual patient identifiers assigned to maintain continuity of care?
  - How are physical bed-tracking and transfer logs maintained?
- **Clinical Documentation**
  - What downtime documentation forms are used for assessments, orders, progress notes, and care plans?
  - How are STAT orders prioritized?
  - How is manual documentation secured and later reconciled with electronic systems?
- **Medication Management**
  - How are medication orders documented using hard copies and manual medication administration records?
  - How is two-person verification performed for high-risk medications during downtime?
  - How does the unit coordinate medication needs with the pharmacy (such as use of landlines, runners, or radios)?
- **Lab and Imaging Coordination**
  - How are manual requisition forms used for lab and imaging orders?
  - How are specimens and imaging requests tracked on paper?
  - How are tests and imaging results communicated manually to clinicians?
- **Patient Monitoring and Safety**
  - What non-networked monitoring equipment is used during outages?
  - How is rounding frequency adjusted to compensate for the absence of electronic alerts?
  - How are critical patients and high-risk areas visually monitored?
- **Staffing and Workflow Adjustments**
  - Who serves as the designated safety officer or downtime coach on inpatient units?
  - How are staff rotations adjusted to prevent fatigue during extended outages?
  - How are staff trained in manual workflows and downtime procedures?

Communication Protocols

- What manual communication tree is used for alerts and coordination?
- Which redundant systems (landlines, radios, runners) are used?
- How are printed contact lists maintained and accessed?

Training and Drills

- How often are outage-related drills conducted?
- How are manual processes practiced (such as use of forms, protocols)?
- How are drills debriefed and policies, procedures, and protocols updated?
- How are contact lists kept current?
- How are new staff trained on outage procedures?

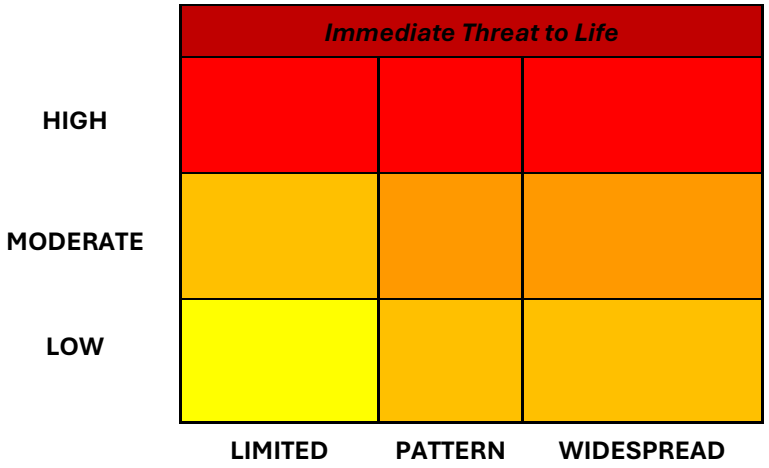
Evidence of Standards Compliance

All noncompliant elements of performance (EPs) will be cited as a Requirement for Improvement (RFI) and will be placed on the *SAFER* Matrix, illustrated below, as determined by the risk level associated with each RFI.

SAFER is the *Survey Analysis for Evaluating Risk* process, a scoring approach used for the CRR program review of health care organizations. *SAFER* is a transformative approach for identifying and communicating risk levels associated with deficiencies cited during the review.

All observations of noncompliance will be documented within the *SAFER* Matrix and require implemented corrective actions that are submitted within the Evidence of Standards Compliance (ESC). The amount of information required within an ESC is reflective of the risk level and associated *SAFER* placement of each RFI.

All RFIs must be addressed via the ESC submission process. The time frame for completing the ESC submission is within sixty (60) calendar days. The organization should work with their Joint Commission account executive to ensure that these submissions are submitted timely.



Survey Analysis for Evaluating Risk (SAFER) Matrix