TIP SHEETS: Please review this page and the Tip Sheets below before submitting your request(s).

- Vendor Risk Assessment Tip Sheet
- Implementation Risk Assessment Tip Sheet (*includes Medical Devices*)

You will need review this page and the tip sheets to familiarize yourself with the updates to have the information needed when completing your request.

External Banner Notice: Risk Cloud is supported by a vendor called LogicGate and you will receive external emails from the logicgate.com domain including "Children's GRC Team <no-reply@logicgate.com>" and "LogicGate Administrator <no-reply@logicgate.com>". These emails will be marked with the external email warning banner. As always, apply secure practices when reading and clicking links from an external sender.

****

What is It & When is a Risk Assessment Required?
An Information Security (InfoSec) Ad Hoc Risk Assessment is required any time a new technology, system, product, service, or device is being considered for implementation or use at Children's. In some cases, introducing significant changes (such as additional functionality or an upgrade) to an existing technology may require an amended RA or a new one.

The appropriate risk assessment(s) **must be completed prior to signing a contract with a vendor or deploying new technology**, unless there is an approved InfoSec Policy Exception allowing for this to occur before the risk assessment(s) is complete. Please reference the 8-23 Information Security Risk Management Policy for more information.

The goal of the RA is to identify and report any security risks associated with the vendor and/or technology and ensure that the implementation of the technology or service meets or exceeds Children's Information Security Policies and Standards (see Policies 8-00 to 8-70).

The Risk Assessment is comprised of:

1. **Vendor Risk Assessment (VRA):** This assessment is meant to review the maturity of the vendor's security practices and the security of the technology, product, and/or services. The IT GRC Team will begin using our new internal solution to assess vendor risks. As needed, an external third-party security risk assessor may be asked to perform the vendor risk assessment.

2. **Technology Risk Assessment:** This assessment could be part of the vendor risk assessment, or the implementation risk assessment done internally by the Children's IT GRC team.

3. **Implementation Risk Assessment (IRA):** This assessment is performed by IT GRC to assess how the new product, technology or service is being implemented into the Children's environment. IT GRC will assess against the controls specified in Children's Policies and Standards and HITRUST Control Framework, and other industry leading security practices.

Timing:

1. The **Vendor and Technology Risk Assessment** can be done prior to or in parallel with the implementation risk assessment. Ideally, it should start before the Discovery Meeting is scheduled or any time a new technology product/service is being considered for purchase.
2. The **Implementation Risk Assessment** portion could be in parallel with the vendor risk assessment if implementation details are known, but it should be done before a project implements the technology, product, or service.
3. Please note that a risk assessment(s) can take 60 to 90 business days to complete. Delays can occur when the vendor does not respond, we don't have security documentation, there is no data flow diagram, and implementation plans are unknown.

Prerequisites for Vendor and/or Implementation Risk Assessments:

- Vendor Risk Assessment
    - Obtain vendor contact (point of contact) information and inform the vendor that we will perform a risk assessment.
    - Applicable vendor supplied security documentation (see **Security Artifacts/ Documentation** table below).
- Implementation Risk Assessment
    - Completed data flow diagram showing how the vendor/technology will interact with Children's staff and systems.

To Get Started:

1. If your effort involves a vendor product or technology service, please submit the Vendor Risk Assessment Request. Please see the Vendor Risk Assessment Tip Sheet.
    - You are able to submit the Vendor Risk Assessment prior or at the same time as the Implementation Risk Assessment. It depends on if your effort knows the details of what will be implemented.
    - The vendor contact information will be needed to answer the security questionnaires. **(Required)**
    - Applicable vendor security artifacts/documentation (see **Security Artifacts/Documentation** table below for list of acceptable documents).
    - *If a vendor is not involved go to the next step.*
2. Requester will complete an Information security Risk Assessment Request with vendor, product, and implementation information. Please see the Implementation Risk Assessment Tip Sheet (*includes Medical Devices*).
    - Data flow diagram(s) showing how the vendor, technology, and services interacts with Children's (see **Basic Data Flow Diagram** or the **Solution Architecture Template** attached to the bottom of this page). **(Required)**
3. The following vendor and implementation information should be made available in the request form:
4. Data flow diagram(s) showing how the vendor, technology, and services interacts with Children's (see **Basic Data Flow Diagram** or the **Solution Architecture Template** attached to the bottom of this page). **(Required)**
5. IT GRC team will contact the requestor to initiate the risk assessment(s) process.

View the Status of the Risk Assessments in our Queue:

- IT GRC follows a First-In First-Out Method (FIFO)
- The GRC Specialist assigned to your RA request, or your IS&T BP can provide you more information on the status of your RA by reviewing our dashboard:
    - IS&T Business Partnering - dashboard

Inquiries/Questions:

- For questions, contact the GRC Specialist assigned to your request.
    - or email the IT GRC Team at IST_IS_GRC@choa.org.
    - or other inquiries, concerns, or escalations contact the Manager, IT Governance, Risk and Compliance (GRC) - Todd Marcinik (todd.marcinik@choa.org), 404-785-5222.

Security Artifacts/Documentation:

Requirement	List of Acceptable Risk Assessment Artifacts
Required	System and network configuration standards - High level architectural design and dataflow diagram (*see template*)
Required	Vendor Contact to work with IT GRC and CORL
Required for Medical Devices	• MDS2 Certification (Manufacturer's Disclosure Statement for Medical Device Security), for medical devices only
Optional-Preferred	A Product Security Overview Document
Optional-Preferred	Most recent AUP, SSAE16 SOC2/Type 2 third-party audit report(s)
Optional	CSA STAR Self-Assessment (Cloud or Co-location specific)
Optional	CSA STAR Attestation (Cloud or Co-location specific)
Optional	CSA STAR Certification (Cloud or Co-location specific)
Optional	SSAE-16 Attestation & SOC 2 Report
Optional	HITRUST CSF Assurance Program
Optional	ISO 27001 Certification or ISO 27002 Self-Attestation including Scope of Applicability
Optional	Executive Summary of certificates held. (e.g., PCI, HIPAA)
Optional	Any product Confidence Report or Vendor Confidence Report
Optional	Security Log Review policies and procedures
Optional	Third party security reviews/assessments/penetration tests
Optional	Application security - Software development and lifecycle (SDLC) process document
Optional	Internal vulnerability assessments of systems, applications, and networks

IS&T Business Partner Matrix:
Please review the matrix below to find the appropriate IS&T Business Partner (BP) liaison. Your IS&T BP can aid with submitting a project or initiative request and help navigate technical implementations.

IS&T Business Partner (BP) Group	Areas of Support	Contact(s)
Revenue Cycle BP	Provides support to the Patient Access areas of Children's on scheduling, registration, referrals, Welcome kiosks, and tablets, RTE (Real Time Eligibility) and ADT (Admit Discharge Transfer, Patient Financial Services on hospital and provider billing/claim/remit workflows and build.	IS&TRevenueCycleAnalysts@choa.org
Business Systems BP	Provides implementation and support to the business side of Children's. (i.e., non-clinical) Departments supported include Supply Chain, Human Resources, Finance/Payroll, Marketing/Communications, Legal/Compliance, Facilities/Security, Engineering, Foundations, Learning Services, and Employee Wellness/Child Wellness.	BusinessSystemsTeam@choa.org
Business Systems BP	Facilities	Andi.Thomas@choa.org
Core Clinical-Hospital Core	Inpatient and Emergency Services.	karl.ellis@choa.org
Core Clinical-Outpatient & Centers	Provides implementation, support & optimization services to CHOA owned Ambulatory practices, Aflac, BMH, Transplant, Ortho, Rehab, Neuro, and CPG/Peds360.	stephnie.cargill-skeeling@choa.org
Ancillary Clinical-Clinical Technology & Integration	Ancillary Services, BMDI/Mobile Clinician, Clinical Partnerships-Marcus, HTM, Credentialing	Steve.Burger@choa.org
Ancillary Clinical-Hospital Ancillary	Surgical Services, Cardiology, Radiology, Imaging, Pharmacy, Clinical Partnerships-Lab	alisha.mathew@choa.org
Patient Digital Experience/Research	Research Support, AccessCHOA, ClockWiseMD, MyChart	Andria.Foerch@choa.org Carol.Price@choa.org

See attachments below for a copy of the ...

- RA process presentation
- Implementation Data Flow Diagram Templates:
  - Basic Data Flow Diagram
  - Solution Architecture
- Tip sheets