Compliance or Chaos: A Research Assessment Survival Guide

Luc Letarte, CIPP/C, CC
Research Cybersecurity and Compliance Specialist

Jessica Galo, CIAPP-P, CC
Research Cybersecurity and Compliance Specialist

LAND ACKNOWLEDGEMENT

What do we do?

- Consultation
- Systems and Security Plan (SSP)
- Security Threat and Risk Assessment (STRA)

Challenges

- Timeline expectations
- Technical information required
- Incomplete information from researcher and vendor
  - E.g. Incomplete scope

Before you start

Be Prepared

- Allocate time
- Designate a contact person
- Understand the scope of your research project
- Cybersecurity language might sound like gibberish and it’s OK!

Don’t go Silo

- Connect with research support groups
- Look for technical and cybersecurity expertise
- Don’t forget your faculty IT team (if you have one)

Don’t go Solo

- Connect with **other** institutions
- Ask the research community
- Connect with organization in your field

Compliance or Chaos

A Research Assessment Survival Guide

Step 1: Summarize your research proposal

- Consider your audience
- Keep it to the point
- Not technical, no worries
- Do not copy paste entire sections of grant proposals/research paper
- Make it about the data, the technology and methodology

Step 2: Identify your data

- What data elements are you working with?
- Does it involve humans?
- Deidentified?
- Linked?
- Is it proprietary?
- **Think about the whole project lifecycle**

Step 3: Classify your data

- Why is this important?
- References:
  - Institutional standards and supplementary materials
    - https://cio.ubc.ca/information-security-standards/U1
    - https://arc.ubc.ca/security-privacy/research-information-classification
  - Alliance standards
    - https://alliancecan.ca/sites/default/files/2022-12/sec_02_en.pdf

Low-Risk Information (Level 1)

Examples:

- Information that requires no protection
- Information that is publicly accessible (e.g. Published annual reports, press releases, new articles)
- Names and work contact information of Alliance Federation Team Members
- Information that may be posted to public websites
- Information of a non-personal and non-proprietary nature including anonymous research data where access to that data is not restricted

Potential risk:

- Minor embarrassment but very limited in scope

Moderate-Risk Information (Level 2)

Examples:

- Proprietary information received from a third party under non-disclosure agreements (NDA) or that we would share under non-disclosure agreements if higher-risk categories are not applicable
- Restricted circulation library journals
- Aggregate financial information and reports
- Technical information about systems or facilities that is unlikely to result in any harm.
- Information of a non-personal, possibly proprietary nature including anonymous research data where access to that data should be restricted

Potential risk:

- Limited impact on reputation or finances within a national host site or affiliate
- Limited impact on operations within a national host site or affiliate
- Loss of priority of publication (e.g. first to publish)
- Loss of access to journals or other copyrighted materials

High-Risk Information (Level 3)

Examples:

- Controlled data requiring protection by law, NDA or industry regulation
- Data associated with patents or patent applications
- Personally identifiable information
- Confidential financial information and records
- Technical information that facilitates compromise of systems or facilities
- Research data that would take significant efforts or cost to collect or reproduce (e.g. additional funding may be required)

Potential risk:

- Impact on reputation or finances of a national host site or affiliate
- Impact on operations of a national host site or affiliate
- Potential for identity theft
- Potential for fraud or spear phishing

Very High-Risk Information (Level 4)

Examples:

- Customer Payment Card Information when a national host site or affiliate is acting in a merchant capacity
- Personal Health Information as defined by provincial or federal legislation (PHI)
- Personally identifiable genetic data
- Biometric data
- Copy of government identification card
- Strategic or sensitive research software or dataset
- Personally identifiable data protected by regulation/legislation (e.g. GDPR)
- Research data that may not be possible to collect or reproduce

Potential disclosure risk:

- Serious impact on reputation or finances of multiple national host sites or affiliates
- Serious impact on operations of multiple national host sites or affiliates
- Financial loss (regulatory fines or damages from litigation)
- Loss of competitiveness of key strategic research area
- Identity theft severely impacting individuals

Step 4: Identify compliance items

- Institutional Standards, Policies and Security requirements
  - Discuss these requirements with your vendor or IT developer.
- Data owner/contractual security requirements
- Privacy/Regulatory/Agreements
- Ethics
- Funding agencies
- **Ask for clarification**

Step 5: Identify solutions involved

- Identify technical resources at the solution provider who can respond to questions architecture, security controls and policies.
- Ask about security based on your requirements
- Review potential solution provider’s ToU/ToS and privacy policy
- Consider the Architecture of the solutions, supply chain and how they fit into your dataflow
- Does it involve AI?
- Using institutionally approved devices where possible simplifies the assessment process

Step 6: Consider the architecture

- Ask for an architecture diagram + detail
- Remember step #4's requirements
- Create a data flow diagram
- Consider storage for active and passive data
- Consider who and how data will be accessed
- Be clear about technical vs administrative controls

Step 7: Think about sustainability

- Who’s providing support and is it in the contract?
- How long will the solution be supported?
- What happens when people leave the team?
- How long is data retained?

Step 8: Hold the vendor accountable

- Inform the solution provider about STRA
- Ask for a demo
- Don’t rely solely on a provider’s certification
- Don't purchase a solution before confirming it meets the requirements **AND** before talking to your procurement dept.
- Challenge information that doesn't match what is advertised
- Ask for specific elements to be in writing

Step 9: Consider responsibilities and accountability

- Shared responsibility model
- Create a RACI chart
- Consider data ownership (eg. Indigenous data)
- Consult before contract signing

Step 10: Create SOPs

- On-Boarding and Off-Boarding procedures;
- User Access review and audit procedure;
- Participant Consent Withdrawal procedure;
- Information transfer and sharing procedures;
- Information backup and restore procedures;
- Maintenance and update/upgrade procedures;
- Vulnerability management;
- Incident response plan

After you receive the STRA report

- Know your gaps, risks, and recommendations
- POAM (Plan of Action and Milestones)

What's a POAM?

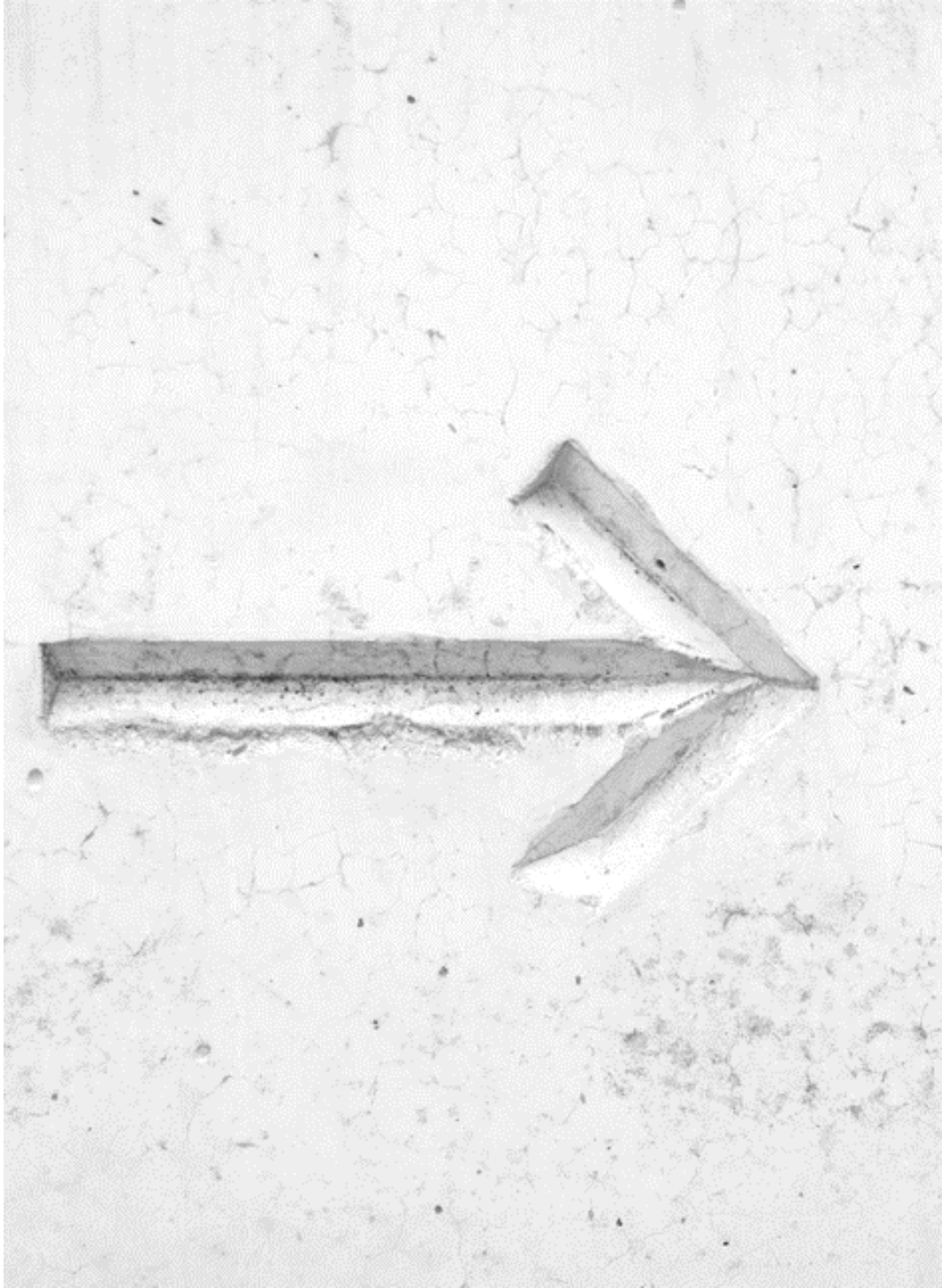
- NIST Glossary Definition:

A document for a system that "identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones."

Source: NISTIR 8286 under Plan of Action and Milestones4 from NIST SP 800-37 Rev. 2 – Adapted

What’s a POAM?

- Document
- Plan to address weaknesses and vulnerabilities
- List of tasks and milestones
- Resources required for completion
- Completion dates for achieving the milestone



After you receive the STRA report

- Know your gaps, risks, and recommendations
- POAM (Plan of Action and Milestones)
- Compliance is Required, not optional
- Variance requests
- Don't panic; there will be gaps

Take Aways

- Start Early
- Documentation should be:
  - Complete
    - Answer the questions instead of just referencing the user guide
  - Clear
  - Consistent
- Don't panic if you can't check a box (a good example is the Data Protection Officer from GDPR)

Q&A

Thank you!

…/in/jessicagalo

…/in/lucletarte

arc.ubc.ca

arc.support@ubc.ca