SRAQ Changelog

Version 1.5

- Responsible Parties:
  - Added Unit Head to table

- Information Classification:
  - Updated table to align with new IS-3 data classification levels
  - Updated the data classification link to match data classification page on security website.

- Risk Classification Calculation
  - Updated to work with the new data classification types (P-Levels and A-Levels)

- System Architecture Diagram:
  - Minor wording changes

- Controls:
  - Minor wording changes - 3.1
  - Made control 4.7 required for High and Medium

Version 1.4

- Minor wording changes and addition of picture upload tools to System Architecture Diagrams section
- Minor wording changes to Controls 2.5, 12.8, 12.11, 12.15, 14.8
- Small formatting change to Identify Threats section

Version 1.3

- Controls
  - Added:
    - 17.4 (secure disposal of physical and digital copies of data)
  - Removed (using old numbering scheme, most of these were replaced by items that are now in Application Security Checklist):
    - 6.2, 6.8, 6.9, 6.12, 6.13, 19.2
  - Minor wording changes:
    - 3.1, 5.5, 6.1, 11.4, 15.1, 16.6
  - Various small formatting changes

Version 1.2

- Risk Classification Calculation
  - It now gives an automatic High rating any time restricted data is reported, regardless of availability/impact/likelihood input.
- Addition of Control 17.1
  - Although it could be implied before from wording on other items, we wanted to make it crystal clear that “Restricted data should be eliminated where possible or must always be encrypted at rest using industry standard strong encryption technologies.”
- Action Plan
  - Addition of Priority column
    - Although before people could infer the prioritization of action items by the target date (something sooner = more important?) that wasn’t always the case, so now it’s easier to communicate prioritization accurately.
    - Increased number of available rows and minor wording changes.
Residual Risk Acceptance

- Completely new section, residual risk is the remaining risk left over after implementing (or choosing not to implement) the safeguards in the Controls section. The purpose of this is that each Control that is required but not fully met should either have an associated action item defined for it in the Action Plan or be formally documented in this new section as an accepted risk by the appropriate risk decision maker. Keep in mind that person is usually the Proprietor / data owner, not the IT person.

Other usability improvements

- Link to data classification help page is clickable.
- Included links to example network diagrams and data flow diagrams (including Visio templates) help page.

Version 1.1

- Main sections are now numbered
- System dropboxes options changed
- Identify Threats section shortened
- Risk Level Calculation tables removed
- Whitespace between controls sections removed
- Various small formatting changes
- SRAQ LITE version created (same document with control detail sections removed)

Version 1.0

- Initial version.