Members: Anne Bilder, Catharine DeRubeis, Natalie Feggestad, Sarah Grimm, David Honma, Lisa Johnston, Jeff Karcher, Lee Konrad, Jeff Korab, Allison La Tarte, Scott Owczarek, Jeffrey Savoy, Mark Sweet, Jack Talaska, Margaret Tennessen, James Yonker, John Zumbrunnen

Attendees: Catharine DeRubeis, Sarah Grimm, David Honma, Lisa Johnston, Jeff Karcher, Lee Konrad, Jeff Korab, Scott Owczarek, Jeffrey Savoy, Jack Talaska, Margaret Tennessen, James Yonker, John Zumbrunnen, Mark Sweet, Tom Jordan, Dan Voeks, Pauline Delfeld, Steve Meyer, Alan Ng, Jon Terrones, Clare Huhn, J.J. Du Chateau, Sara Hagen, Jonathan May, Chris Richards, Steve Tanner, Steve Devoti, Phil Hull

Data Governance Council Meeting Minutes
Tuesday, August 15, 2023
8:30-10 a.m.

Agenda

1) 8:30 - Near final data integration standard for DGC input (Tom Jordan/Subcommittee)
   a) This standard was an identified need from the IDP for how institutional data can be integrated into applications
   b) Tom listed members from charter and presented standard
      i) Goals
      ii) Definitions
      iii) Integrations Catalog - meant to help campus understand the various integration products available to them
      iv) Use of data in integrations helps users understand their role
      v) Integrations Registry - Providers should be able to document the users of their integration products to be
         able to communicate any changes, downstream impacts. Also need to understand the criticality of these
         integrations, if broken, can business still function?
      vi) Vendors and third parties
      vii) Implementation recommendations
         (1) This standard is focused on data, not technology or IT practice. There is a need for a group to provide
         guidelines for the IT practice to implement this integrations standard.
         viii) Next steps
            (1) Jeff Savoy: Seek feedback from DOIT directors to get feedback.
            (2) JJ.: Get this to ITCCC to help define the impacts to their systems.

2) 9:00 - Gender data use guidelines (Core Person Data Operations Team) - request for feedback on next steps for campus input
   on draft guidelines
   a) RO can help provide a list of the admitting offices
   b) Present to Enterprise Data Gov Council (UW Sys)
   c) System configurations may need to be changes
   d) CAOS needs to be on the list

3) 9:30 - Smart Access (ZeroTrust principles) - investigating Microsoft products (best of suite vs best of breed) - Jeff
    Savoy/Steve Tanner/Jonathan May/Steve Devoti (30m) (and Chris Richards)
   a) Jeff:
      i) Goal: Raise awareness of Smart Access. Based on Zero Trust principles
      ii) Problems: Treat landscape, attackers breaking into a system. Reduce the blast radius, detect compromises.
         Keep breaches short term, close them fast.
      iii) Higher visibility of our security posture, personally owned devices, including mobile, but also respecting
         privacy
      iv) Remote work. Untrusted networks at home. Reduce these problems
   b) Steve:
      i) Smart Access is based on zero trust principles. NIST 800-207.
      ii) Not a thing you buy, but tenets and principles that inform the architecture, capabilities to support those
         principles
      iii) Rebrand “zerotrust” as “Smart Access”
         (1) Assume breach. Isolate. Minimize the blast radius.
         (2) Visibility. Getting more data to analyze and understand what's happening in your systems
         (3) Least privilege access. Need to re-eval ongoing. Just enough access, just in time. Not just access, but
         does your machine have all the needed security measures, patches, etc.
      iv) Guiding Principles
         (1) Meet university needs
(2) Enhanced security posture
(3) Reduced integration complexity - pieces need to talk to each other
(4) Efficient use of university resources (licensed solutions; iterative approach; focus on areas with the most risk)

v) Microsoft platform selected. They do identity management well, and have all the security tools for servers, etc. They can also provide the data we need to address zero trust.

c) Jonathan:
i) Reduce the number of IT vendors. Use Microsoft. May also need other partners.
ii) Lots of tools (see slides)
iii) Microsoft Azure Purview - data governance system.
   (1) Compliance manager - assess risks and controls with various industry controls and regulations, audit reports.

d) Steve:
i) User experience drives decisions.
ii) Trying to access sensitive or restricted data outside of regular business hours, ask for MFA again.
iii) Looks at all data points, analytics, in real time, to help manage the risk.
iv) Just starting this project. Can't do everything all at once.
v) 2023 - Tech viability, go/nogo
vi) 2024 - do pilots, refine, service launch

e) Jeff: https://website gi.wisc.edu/smartaccess

f) Questions
i) Mark: How does smart access intersect with controlled unclassified information / NIST 800-171
ii) Dan: Microsoft purview
iii) Lisa: Connections to data gov
   (1) Software - gov tool
   (2) Data stewards, classification, access authorization
   (3) Privacy/surveillance
iv) Jeff Karcher: Business case for our insurance, could update that.

4) Updates
i) Search launched for an Office of Compliance Assistant Director of Data Privacy and Transparency (David H., Scott O., Lisa J. are the DGC council members on the committee)
ii) DAPIR will be recruiting for a Director for Institutional Research and & Decision Support
iii) DIMP: Jul 25th Peter Kinsley (Grad School) reported missing data in the InfoAccess data view: Bursar Assessed Tuition for fiscal years 2022 & 2023