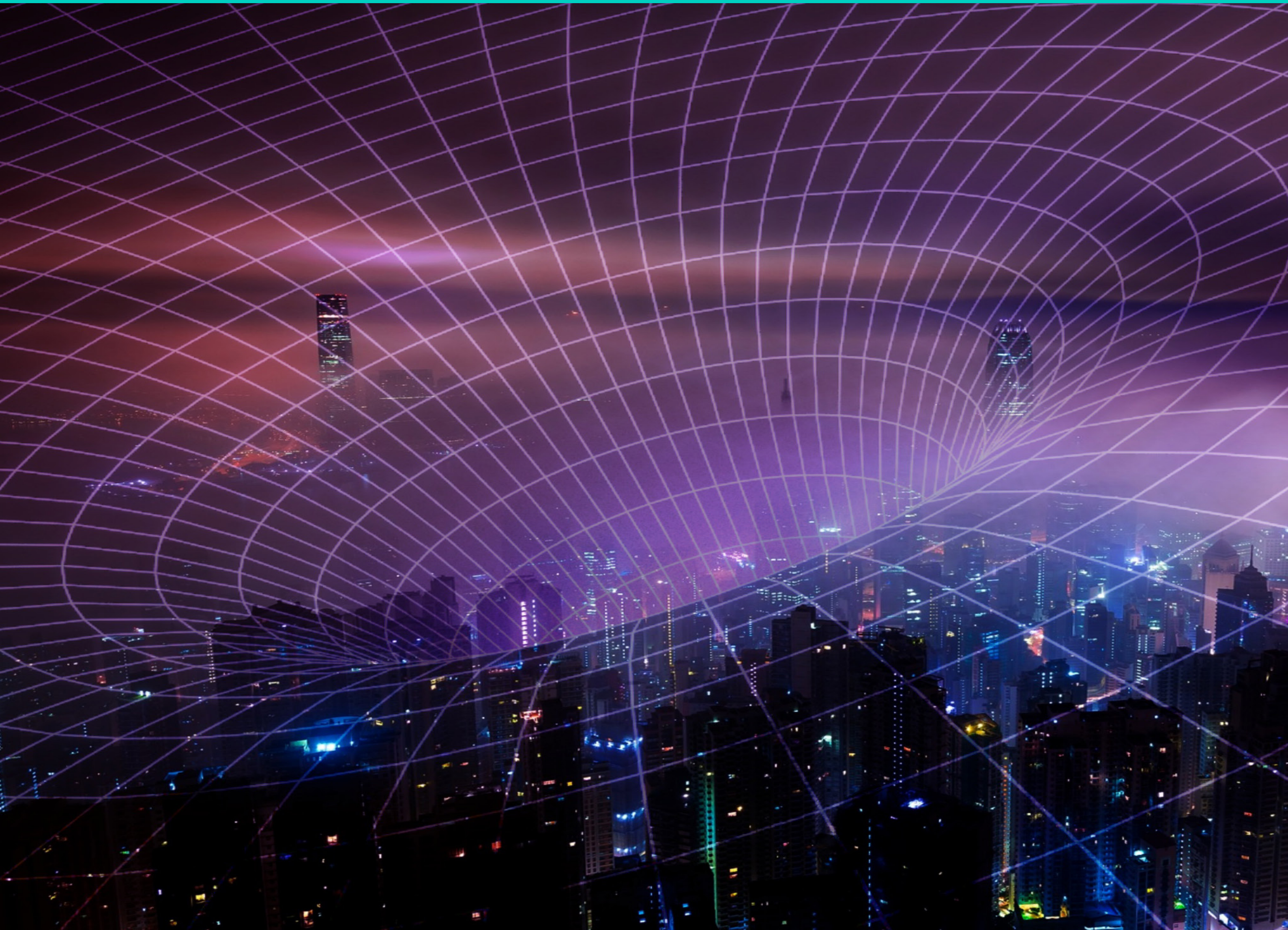
How to Quickly Close Cybersecurity Risks Today and Produce an Identity Strategy for the Future

WORKBOOK



Book a Meeting

Schedule a follow up meeting to talk about how you tackle next steps for your team.

SCAN

VISIT www.bravurasecurity.com/downloads

Table of Contents

10 Step Process to Modernize IGA in Higher Education

1. **Identify Stakeholders:** This includes key stakeholders, but also extended stakeholders. Typically, this includes people from the following areas:

- Registrar's Office
- Human Resources
- Enrollment Systems
- Undergraduate Admissions
- Support teams (this includes any support teams for faculty, staff, students, alumni, and any others). Holding workshops with these support teams will give a lot of insight on where the University's constituents are having difficulty. This is a great source to start documenting where the gaps are in the existing systems/processes
- Information Security Office
- Data Stewards
- Technical Subject Matter Experts from the enterprise systems in use today at the University
- Consumers of any of the technology services today which are being replaced as part of this project.

Workshops should be conducted with each of the respective identified stakeholders to collect information related to the technical integration as well as the business processes that support the system (as it relates to Identity Lifecycle Management). Ensure that you solicit feedback on the as-is systems and processes with all stakeholders as each group may have a different perspective on what is working well, what gaps may be present, and where people struggle.

2. **Technical Assessment of Existing Services/Products:** This will take a fine-grained look at the existing technical solutions today which are responsible for providing Identity and Access Management. If documentation does not currently exist, or is out of date, this should be remediated. This includes documenting the technical functionality provided by the component as well as any business logic which may be built into the system(s). Typically, the best person to document the technical components is the person who is closest to it, whether they are the developers, maintainers and/or owners of the application

A. Document all interfaces and interconnected systems with as much detail as possible.

B. Any logic contained within the system should be graphically documented in a flowchart; such that it is easy to understand what the system is doing and any business rules or logic. This can later be used while building the future state architecture,

C. Identify and document any technical requirements as you are documenting the technical capabilities of the system/component. Note: a sample requirements document has been provided along with this report for reference.

D. Develop a logical and physical architecture diagram of the system, and interconnected systems. It is also very useful to maintain an overall logical and physical architecture diagram outlining the entire landscape of systems which communicate, and transfer data related to Identity Lifecycle Management

E. Create a web-based survey which can be sent to a vast audience of extended stakeholders to rate the overall lifecycle management experience of constituents to the University. The survey should be written in such a manner as to solicit feedback about the services that are being replaced today. For each topic, a linear scale question would indicate how satisfied they are with the topic, and a paragraph answer question would allow them to indicate why they may be satisfied or dissatisfied with the item. Example topics are provided below:

- Account Claiming Process
- Account Creation
- Account Management
- Password Recovery
- Username Recovery
- Access Request for supplemental access
- Any other self-service capabilities
- Termination Process
- Any others

F. Identify any design considerations while you are working through this and make note of anything which may impact the design. Keep a running tab of these as you are working through the different functional areas.

G. Consumers: Identify any consumers of the data for the system which you are assessing.

3. **Document Requirements:** Functional and Non-Functional requirements should be documented prior to engaging with IAM product vendors.

4. **Identify Use Cases:** This is just the process of identifying all of the various use cases that are facilitated by the components listed above and their feed integrations. At this stage the main goal is to just identify the use cases. The detailed use cases will be developed after the appropriate workshops and information gathering has been completed. Included as part of this report, you will find a sample use-case document which was developed by another University for a similar project, note: data has been scrubbed, however it should be a good starting place to identify the types of use-cases which need to be documented.

5. **Business Process Assessment:** This will take a fine-grained look at the existing business processes which have an impact on technologies. Any business processes which are not formally documented should be documented.

   Workshops should be conducted with the various people responsible for each distinct user population. For example: Human Resources will be able to help you identify the processes related to onboarding faculty/staff, as well as transfers and terminations (immediate and scheduled). Workshops should be conducted with all parties involved in the process. Sample questionnaires are also provided in the corresponding package included in this report. These workshops will assist in building out the details of each of the use cases which were identified in step 2. Each use case should be well documented along with any alternate steps/processes and should have a corresponding use-case diagram to help illustrate it. This will help tremendously when designing and building the new solution. It will help the implementation team understand how the system must behave and what the expected outcomes are.

6. **Policy Assessment:** Examine existing policies related to Identity and Access Management as well as identify policies which are not present. It is best practice to put University-wide policies in place before building the future state solution. This will allow for a much less complex IGA deployment with streamlined policies across the board.

7. **Gap Analysis:** Document areas of deficiencies, and areas for improvement to overall end-user experience. As you are conducting your workshops, solicit feedback from all key and extended stakeholders about what works well and what does not. Keep a running list of the identified gaps or problem areas. It is more than likely possible that you will be able to solve many of areas of deficiencies with the new platform. This will also encourage a favorable view of the overall project as you are deploying the new solution.

8. **Key Performance Indicators:** Define key performance indicators to measure the success of the new system(s).

9. Request for Proposal / Vendor Selection: In our experience, we find that it is best to split the RFP into multiple RFPs for the following functional areas:

- Identity Governance and Administration
- Web Access Management/Federation (or CASB solution if that is a better fit)
- Privileged Access Management.
- Multi-Factor Authentication

The reason why we split this out into multiple key areas is because in our experience there are no one solution-fits all vendors. While there are several vendors that have solutions that include all these functional areas, some vendors may not respond to an all-inclusive RFP since they do not offer every one of these technologies. However, it is important to note that you should include integration options of these technologies into the Identity Governance and Administration track (meaning that there are integration options between Privileged Access Management and Multi-Factor Authentication solution).

In this workstream the vendor selection scoring and selection process should be well documented. Please also refer to Gartner's Evaluation Criteria for Identity Governance and Administration toolkit, which is a great collection of requirements that span all capabilities of these platforms.

10. Implementation Planning / Roadmap: Execution of the RFP's and vendor bake-offs. This should include product demonstrations as well as on-premises proof of concepts for the final contenders. Identify quick wins (high-impact, low-risk) to determine sequencing and develop a roadmap.

Example Use-Cases

1. Onboarding Use-Cases

a. Initial Bulk Load from Legacy IdM
b. Onboarding new Employee from HR
c. Onboarding new Student from SIS
d. Record Matching
e. Manual Record Matching
f. Conflict Resolution
g. New Identity Creation
    i. Username generation
    ii. Campus ID assignment
    iii. GUID generation
    iv. Account Claiming process

2. Re-activation

a. Affiliation based
b. Temporary re-activation

3. Update Use-Cases

a. Identity data update record from HR
b. Identity data update from SIS
c. Identity data update from others

4. Birthright Provisioning Use Cases

a. Role assignment
    i. Account provisioning
    ii. Entitlement provisioning
b. Role removal
    i. Account de-provisioning / disablement
    ii. Entitlement removal / disablement
c. Based on affiliations
    i. Staff
    ii. Student
    iii. Faculty
    iv. Staff
    v. Alumni

vi. Emeritus

vii. Sponsored

viii. Others

5. Separation Use-Cases

a. Scheduled Termination - Faculty / Staff / Others

b. Immediate Termination - Faculty / Staff / Others

c. Faculty / Staff goes on LOA

d. Faculty / Staff returns from LOA

e. Student becomes Alumni

f. Student leaves the university

6. Password Management

a. Initial password creation for accounts

b. Password change - self-service

c. Forgotten password

d. Password synchronization

7. Access Request and Approval

a. Request process

b. Who can request what, and for whom?

8. Approval process

a. Escalations

b. Expirations

c. Notifications

9. Fulfillment

10. Temporary access (Sunrise/Sunset)

11. Access Certification

a. Schedule based

b. Event driven (i.e; departmental transfer)

c. Approval, escalation, expiration and notifications

Sample Detailed Use-Case

Number:	1
Title:	Onboarding new Employee from Banner HR
Created By:	Business Analyst
Date Created:	OCT 25, 2021
Last Updated By:	Business Analyst
Date Last Updated:	OCT 5, 2022
Action Initator:	Human Resources (Data entry)
Affected Personnel:	N/A
Description:	This purpose of this use case is to load the new IGA tool with existing Identity Data.
Preconditions:	• HR Personnel utilize the lookup to search for a previous instance of the person in the IGA system. If the person is found, the campus username is set in Banner. If not, it is left blank, the IGA system will generate a new username and send back to Banner. • HR entered the new hire information into Banner HR and assigned a position to the user along with start date.
Normal Flow:	1. IGA system executes the Banner HR synchronization task which queries the Banner HR IGA view for the full set of employee zrecords. 2. The IGA system evaluates each record to determine if it matches against an existing record via the HR unique identifier. 3. If unique identifier matches, the system will perform a pre evaluation on the record to see if any values have changed, if not it will ignore the event and this process stops; if the values have changed then the system will submit a change event and the flow will continue at step 5 4. If a unique match was not found the system will process the record through the record matching engine which will result in one of three responses: Match, No Match, or Research a. Match will process the changes against an existing user and will continue to step 5 b. No-Match will process the event as a new record using the “New IGA System Record Creation” process and this flow will continue to step 5. This will also generate a new username and send that back to Banner. c. Research will keep the record as an unmatched event for manual intervention. 5. The IGA system record will be evaluated in the context of the sets of attributes. 6. The IGA system record will be updated/created from the data in the event and the attributes will be evaluated by the role assignment logic to assign the record to system roles based on attribute values. 7. Any accounts and entitlements which are provided by roles assigned are provisioned for the user. 8. If the record is new the account claiming process will be initiated (process may be specific based on department). 9. Any HR related downstream systems would be updated with the new information.
Exceptions:	N/A
Importance:	High
Frequency of Use:	4 times daily
Business Rules:	Access provisioning needs to be triggered for new workers.
Special Requirements:	N/A
Assumptions:	N/A
Notes & Issues:	N/A
Business Areas:	Users
Expected Outcome:	New members of the workforce are automatically granted basic access.
Related Use Cases:	Use Cases 5,9, and 18.

Authoritative Source: Data Stewards Questionnaire

Workshop Group

The following questions are broken down by category, all questions may not be applicable to all functional areas.

Technical Questions

1. What is the Application Name / Vendor / Version where your data resides?

2. Are there any planned changes to your application? Migrating to a new application? Planned upgrade? Etc.

3. Describe the type of application. What is the backend repository? How are users authenticated into the system? What provides authorization to the system?

4. What types of API's are available to get access to your data (REST, SOAP, Vendor Provided API, etc.)?

5. What environments are available (i.e.; DEV, Test, QA, UAT, Prod etc.)? Where are they physically located? Is the data in the pre-production environments representative of production data? How often are the lower environment refreshed?

6. Are there any logical or physical diagrams of the infrastructure that may be shared?

7. Does any process flow related documentation exist regarding your system's data that can be shared? How does data flow into the system?

8. What are the current number of users listed by "type" in your system today i.e. number of employees/ contractors/vendors/students etc.)?

9. For each of the user types, what information do you currently store? Can you share the list of data elements that is stored by each type as well as what fields are mandatory, and which are optional as well as which ones may be multi-valued?

10. What information is eligible to be made available to Identity Services for consumption?

11. Do people have a self-service interface for updating their personal information? If not, what is the process for people to update their information?

12. How do users get access to your application? Who requests the granting of access? How do they request access? Who approves access? Who is eligible to have access? What is the approval process for granting access?

13. How is access currently revoked? Who requests the revocation of access? Who approves the revocation of access? What measures are taken to ensure that only the people who are eligible have access?

14. When someone becomes in-eligible for access (such as an employee termination) what triggers the revocation of access?

15. What is current number of active users/accounts in the system?

Technical Questions

16. How does your system currently integrate with Identity Services? Please describe any existing integrations.

17. What are your general thoughts regarding the current integration? Are you satisfied with how things work today? What improvements can be made to improve the process and/or end user experience?

18. Are there any restrictions which would prohibit Identity Services from integrating with your system? If so, what are they?

19. Are there any pieces of information which Identity Services provides which your system consumes? How is that done today? Are there any restrictions for changing the method? Are there any desired changes to this?

20. Do you currently utilize any services provided by Identity Services for your own needs? If so, what are they? What types of data do you consume from Identity Services?

21. What are your general thoughts regarding these services/data? Are you satisfied with how things work today? What improvements can be made to improve the process and/or end user experience?

22. Can you think of anything else pertaining to our project that would help from an end-user experience or process perspective?

Graduate Departments Questionnaire

Workshop Group

The following questions are broken down by category, all questions may not be applicable to all functional areas.

Technical Questions

1. Please describe the graduate admissions process. At what point in the process does the student become eligible for access to university resources?

2. What information is entered for an accepted student? What personal contact information is collected?

3. What happens when a student does not show up? Is the transaction rolled back, or does the student's status change?

4. Are there any differences in process for a new graduate student vs. a student who has either been previously enrolled at the university?

5. Under what conditions does a student's eligibility for access to resources change? What are the triggers in the system for this status change? What are the triggers which change the student's status to Alumni?

6. Do students have the ability to update their personal information via Self Service? What information are they allowed to update, and are there any approvals?

7. Are there any other initiatives/changes that we should be aware of that may affect our project? Planned upgrades? Process changes?

8. Do you currently utilize any services provided by Identity Services for your own needs? If so, what are they? What types of data do you consume from Identity Services?

9. What are your general thoughts regarding these services/data? Are you satisfied with how things work today? What improvements can be made to improve the process and/or end user experience?

10. Can you think of anything else pertaining to our project that would help from an end-user experience or process perspective?

HRIT Questionnaire

1. Please describe the new-hire process. How does a candidate transition to an employee and at what point is the new hire information entered into the HR system in relation to their actual start date?

2. What information is entered for a new hire? What personal contact information is collected?

3. What happens when a new hire does not show up for work? Is the transaction rolled back, or is the employee record terminated?

4. Are contingent workers/contractors managed in the HR system? If so, what differences exist between the handling of employees vs. contingent workers/contractors?

5. Does a leave of absence change the employee status? Does this change their eligibility for access?

6. Please describe the standard termination process. Who initiates the termination, and at what point in relation to the actual termination date is the termination entered into the HR system?

7. Please describe the immediate termination process. Who initiates the termination, and at what point is this captured in the HR system? What steps are taken to immediately terminate access to university resources?

8. If contingent workers/contractors are managed in the HR system, please describe the process in which an employee transitions to a contingent worker/contract or vice-versa. Do they retain their old employee identifier? Is the old record terminated first? Is the new record created at the same time?

9. For employees which have more than one job assignment are there any identifiers for Identity Services to understand which is the primary job assignment?

10. Do employees have the ability to update their personal information via Self Service? What information are they allowed to update, and are there any approvals?

11. Are there any other initiatives/changes that we should be aware of that may affect our project? Planned upgrades? Process changes?

12. Do you currently utilize any services provided by Identity Services for your own needs? If so, what are they? What types of data do you consume from Identity Services?

13. What are your general thoughts regarding these services/data? Are you satisfied with how things work today? What improvements can be made to improve the process and/or end user experience?

14. Can you think of anything else pertaining to our project that would help from an end-user experience or process perspective?

Information Security Office Questionnaire

1. What policies exist university wide related to having access to university resources? Are these policies ocumented and available? Are they well known?

2. What guidelines exist university wide related to having access to university resources? Are these policies documented and available? Are they well-known?

3. What policies/guidelines exist for data classification/data protection?

4. What is the current policy/guideline related to audit/logging of events related to IAM (account lifecycle management events)?

5. What is the current policy/guideline related to audit event retention?

6. What is the current process/policy related to an immediate termination event?

7. What is the current process/policy related to account re-activation?

8. Are there any policy/guidelines (pertaining to services which Identity Services provides) which are subject to change in the near future? Or any discussions of change?

9. Are there any gaps that you are aware in the existing IAM infrastructure/services which do not meet university wide policy and/or guidelines?

10. Are there any changes; from your perspective, that you would recommend related to our project which we should take into consideration as we decide on a future state for IAM services?

11. Are there any other initiatives that we should be aware of that may pertain to our project?

12. Do you currently utilize any services provided by Identity Services for your own needs? If so, what are they? What types of data do you consume from Identity Services?

13. What are your general thoughts regarding these services/data? Are you satisfied with how things work today? What improvements can be made to improve the process and/or end user experience?

14. Can you think of anything else pertaining to our project that would help from an end-user experience or process perspective?

Library Questionnaire

Workshop Group

1. Do you currently utilize any services provided by Identity Services for your own needs? If so, what are they? What types of data do you consume from Identity Services?

2. What are your general thoughts regarding these services/data? Are you satisfied with how things work today? What improvements can be made to improve the process and/or end user experience?

3. Can you think of anything else pertaining to our project that would help from an end-user experience or process perspective?

Staff Department Initiators Questionnaire

1. Please describe the new-hire process. How does a candidate transition to an employee and at what point is the new hire information entered into the HR system in relation to their actual start date?

2. What information is entered for a new hire? What personal contact information is collected?

3. What happens when a new hire does not show up for work? Is the transaction rolled back, or is the employee record terminated?

4. 4. Are contingent workers/contractors managed in the HR system? If so, what differences exist between the handling of employees vs. contingent workers/contractors?

5. Does a leave of absence change the employee status? Does this change their eligibility for access?

6. Please describe the standard termination process. Who initiates the termination, and at what point in relation to the actual termination date is the termination entered into the HR system?

7. Please describe the immediate termination process. Who initiates the termination, and at what point is this captured in the HR system? What steps are taken to immediately terminate access to university resources?

8. If contingent workers/contractors are managed in the HR system, please describe the process in which an employee transitions to a contingent worker/contract or vice-versa. Do they retain their old employee identifier? Is the old record terminated first? Is the new record created at the same time?

9. For employees which have more than one job assignment are there any identifiers for Identity Services to understand which is the primary job assignment?

10. Do employees have the ability to update their personal information via Self Service? What information are they allowed to update, and are there any approvals?

11. Are there any other initiatives/changes that we should be aware of that may affect our project? Planned upgrades? Process changes?

12. Do you currently utilize any services provided by Identity Services for your own needs? If so, what are they? What types of data do you consume from Identity Services?

13. What are your general thoughts regarding these services/data? Are you satisfied with how things work today? What improvements can be made to improve the process and/or end user experience?

14. Can you think of anything else pertaining to our project that would help from an end-user experience or process perspective?

Support Teams Questionnaire

Workshop Group

1. What types of users do you support?

2. What types of systems/accounts do you provide support for with your userbase?

3. What are the different types of issues do users contact you for assistance?

4. Of these types of issues, which have the highest volume of? Do you have any statistics which can be shared with the project team?

5. What would you consider the major issues? From your perspective what could be done to improve this?

6. What types of issues make a bad user experience for your user base? From your perspective what could be done to improve this?

7. Do you currently utilize any services provided by Identity Services for your own needs? If so, what are they? What types of data do you consume from Identity Services?

8. What are your general thoughts regarding these services/data? Are you satisfied with how things work today? What improvements can be made to improve the process and/or end user experience?

9. Can you think of anything else pertaining to our project that would help from an end-user experience or process perspective?

Undergraduate Admissions Questionnaire

1. Please describe the undergraduate admissions process. At what point in the process does the student become eligible for access to university resources?

2. What information is entered for an accepted student? What personal contact information is collected?

3. What happens when a student does not show up? Is the transaction rolled back, or does the students status change?

4. Under what conditions does a student's eligibility for access to university resources change? What are the triggers in the system for this status change? What are the triggers which change the student's status to Alumni?

5. Do students have the ability to update their personal information via Self Service? What information are they allowed to update, and are there any approvals?

6. Are there any other initiatives/changes that we should be aware of that may affect our project? Planned upgrades? Process changes?

7. Do you currently utilize any services provided by Identity Services for your own needs? If so, what are they? What types of data do you consume from Identity Services?

8. What are your general thoughts regarding these services/data? Are you satisfied with how things work today? What improvements can be made to improve the process and/or end user experience?

9. Can you think of anything else pertaining to our project that would help from an end-user experience or process perspective?

Next Steps

Schedule a follow up meeting to talk about how you tackle next steps for your team.

SCAN

VISIT www.bravurasecurity.com/downloads

We Are Bravura Security

For 30 years Bravura Security has helped many higher education institutions achieve incremental Identity Governance and Access Management success. Bravura Security, an analyst-recognized leader, delivers decades of experience and the industry's only single Identity, Privileged Access, Password and Passwordless management platform, the Bravura Security Fabric. This end-to-end platform offers users a robust and frictionless security experience, governance and compliance checks, and streamlined service-level agreements via a single platform, which further decreases overall risk and lowers total cost of ownership for deployment and administration.

Bravura Security, Inc.

Corporate Headquarters
1401 - 1st Street S.E., Suite 500
Calgary, Alberta, Canada T2G 2J3
bravurasecurity.com

Contact Information
1.403.233.0740
Sales Toll Free: 1.877.386.0372 / 1.877.495.0459
sales@BravuraSecurity.com