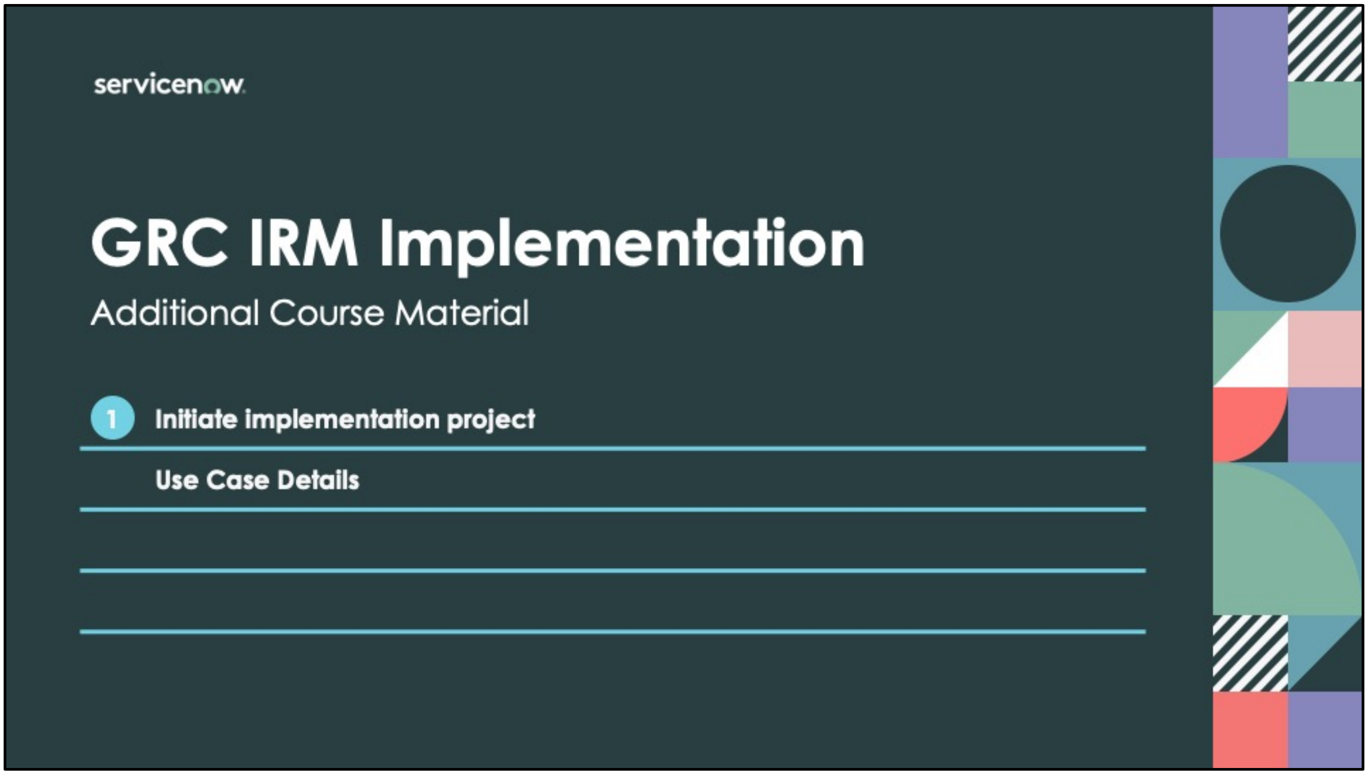


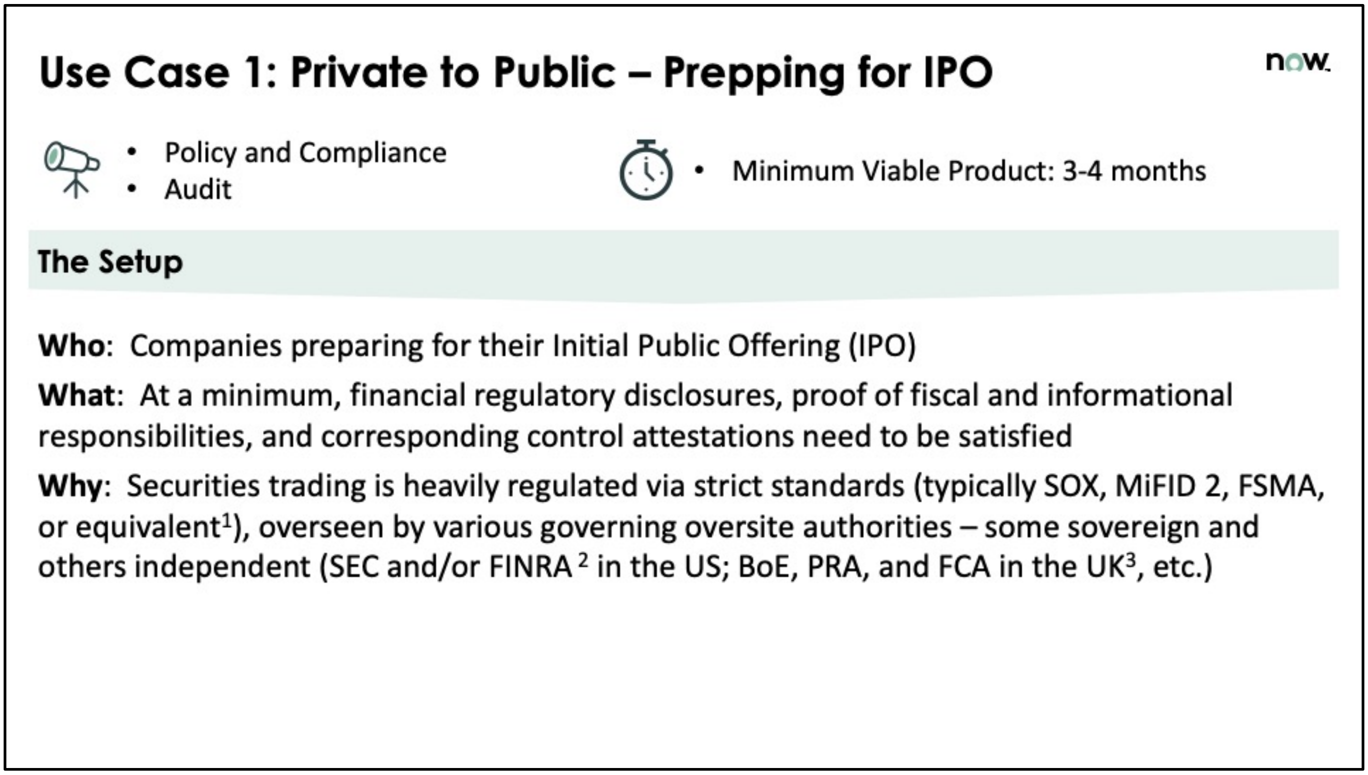
servicenow

GRC IRM Implementation

Additional Course Material

1 Initiate implementation project

Use Case Details



Use Case 1: Private to Public – Prepping for IPO

- Policy and Compliance
- Audit

- Minimum Viable Product: 3-4 months

The Setup

Who: Companies preparing for their Initial Public Offering (IPO)

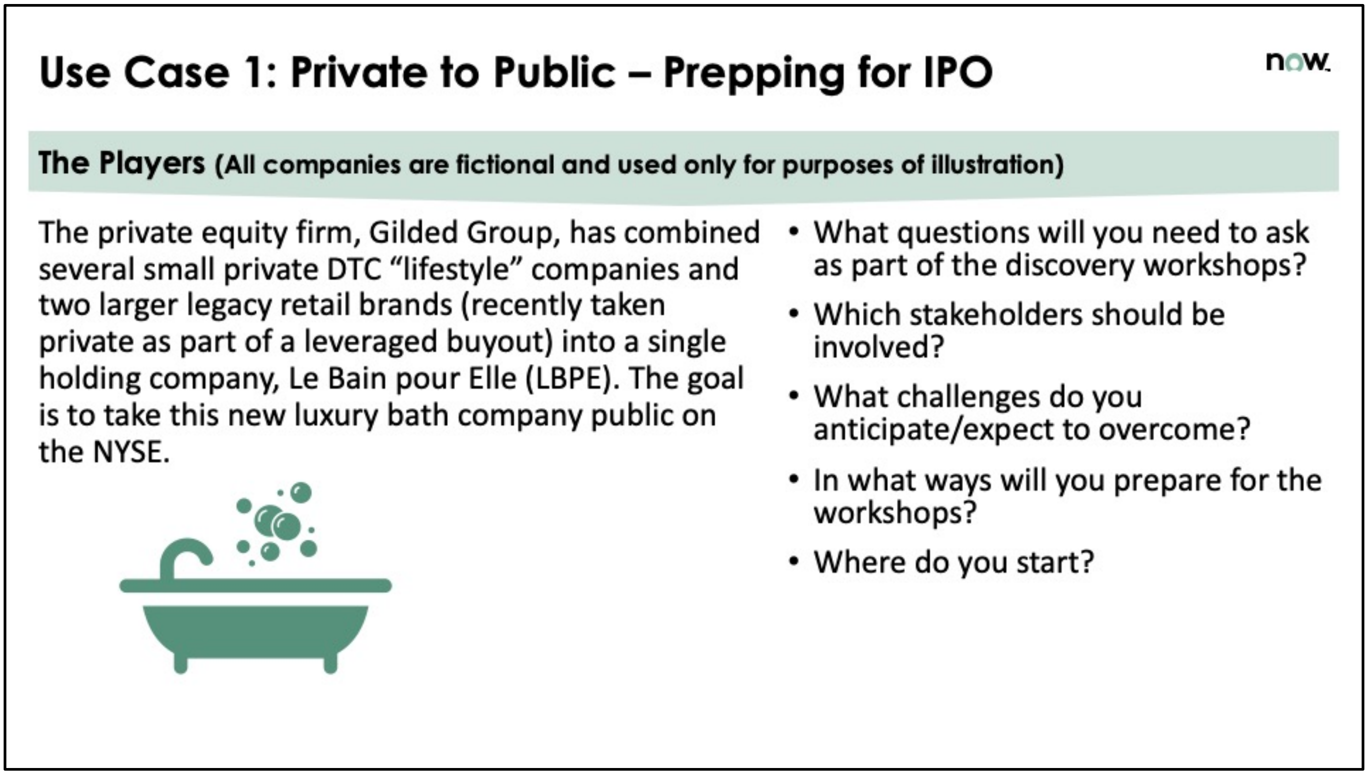
What: At a minimum, financial regulatory disclosures, proof of fiscal and informational responsibilities, and corresponding control attestations need to be satisfied

Why: Securities trading is heavily regulated via strict standards (typically SOX, MiFID 2, FSMA, or equivalent[1]), overseen by various governing oversite authorities – some sovereign and others independent (SEC and/or FINRA [2] in the US; BoE, PRA, and FCA in the UK[3], etc.)

[1] Sarbanes-Oxley in the US, Markets in Financial Instruments Directive 2014 in the EU, Financial Services and Markets Act 2000 in the UK, respectively.

[2] The Securities and Exchange Commission the US Governmental Agencies with jurisdiction over financial instruments offered by companies and/or the Financial Institution Regulatory Authority the body which certifies and licenses securities brokers.

[3] The Bank of England, which is the governing body over both the Prudential Regulation Authority and the Financial Conduct Authority – all three together share the responsibility of overseeing Authorisation, Prudential matters, and the Conduct of business in the UK.



Use Case 1: Private to Public – Prepping for IPO

The Players **(All companies are fictional and used only for purposes of illustration)**

The private equity firm, Gilded Group, has combined several small private DTC “lifestyle” companies and two larger legacy retail brands (recently taken private as part of a leveraged buyout) into a single holding company, Le Bain pour Elle (LBPE). The goal is to take this new luxury bath company public on the NYSE.

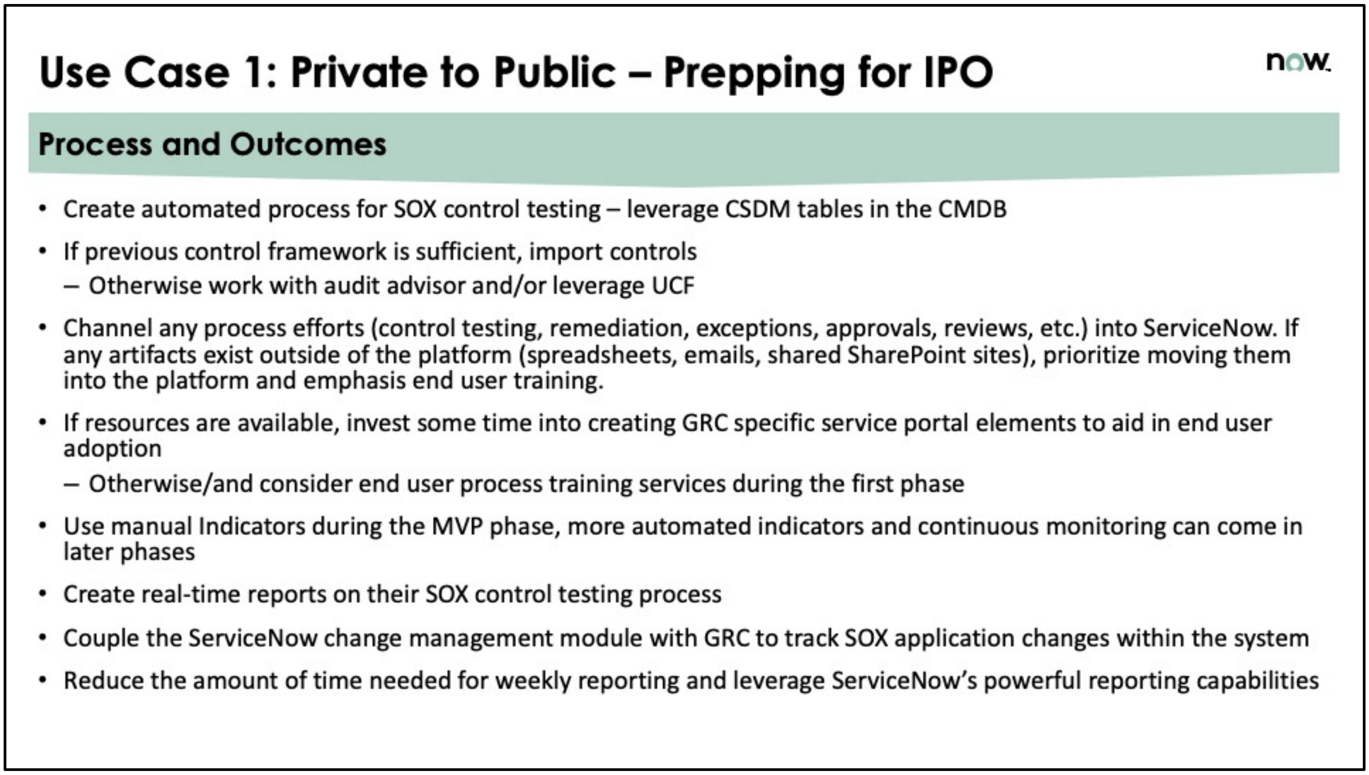
- What questions will you need to ask as part of the discovery workshops?
- Which stakeholders should be involved?
- What challenges do you anticipate/expect to overcome?
- In what ways will you prepare for the workshops?
- Where do you start?

Scenario 1: A private equity firm (Gilded Group) has purchased a variety of small to medium sized companies, most are newer Direct to Consumer (DTC) and “Life Style” brands that have aged beyond their startup phase, have built a loyal following, and have decent re-occurring revenue streams, but just haven’t developed into companies that would make an attractive IPO investment. Additionally, two older legacy brands (Son Bain and CandleShoppe) that had recently fallen on harder times and/or failed to navigate the transition in retail away from shopping malls have also been scooped up via a leveraged buy out (LBO). The legacy companies were stripped of useful brand, retail real-estate, and intellectual property assets with a core group of management and talent being kept on with the new entity. All other assets were sold as part of the buyout and process of taking the firms private.

The best remaining assets have been transferred and consolidated into a single corporate entity, using the most widely recognized and respected legacy brand (Son Bain) at the core of a new limited holding company. Son Bain has been rehabilitated for a new generation and is now known as Le Bain pour Elle (a Son Bain Ltd company). LBPE offers a compelling set of tiered subscription bundles to customers directly, and a handful of prime “flagship” physical locations has been remodeled to offer an in-person lifestyle (Indulgence as Self Care!) experience.

Gilded Group has already done the advisory work of helping to rebuild the company completely and 14 months later is ready to get the IPO show on the road. They’ve provided policy and control guidance based on templates they’ve used previously to help LBPE prepare for their SEC filing and disclosure. They’ve approached your team about implementing ServiceNow GRC (Policy and Audit) to help LBPE prepare for IPO and beyond. During the re-org, LBPE’s new IT department implemented ServiceNow ITSM for their helpdesk services and has recently begun the process of using Discovery and Software Asset Management for in-house assets, but this is being implemented by a different team and will not be ready for 6-9 months. All other infrastructure and services reside in AWS (marketing, retail store services, website services, etc.).

This implementation must be ready for Go Live within 3 months.



Use Case 1: Private to Public – Prepping for IPO

Process and Outcomes

- Create automated process for SOX control testing – leverage CSDM tables in the CMDB
- If previous control framework is sufficient, import controls
  - Otherwise work with audit advisor and/or leverage UCF
- Channel any process efforts (control testing, remediation, exceptions, approvals, reviews, etc.) into ServiceNow. If any artifacts exist outside of the platform (spreadsheets, emails, shared SharePoint sites), prioritize moving them into the platform and emphasis end user training.
- If resources are available, invest some time into creating GRC specific service portal elements to aid in end user adoption
  - Otherwise/and consider end user process training services during the first phase
- Use manual Indicators during the MVP phase, more automated indicators and continuous monitoring can come in later phases
- Create real-time reports on their SOX control testing process
- Couple the ServiceNow change management module with GRC to track SOX application changes within the system
- Reduce the amount of time needed for weekly reporting and leverage ServiceNow's powerful reporting capabilities

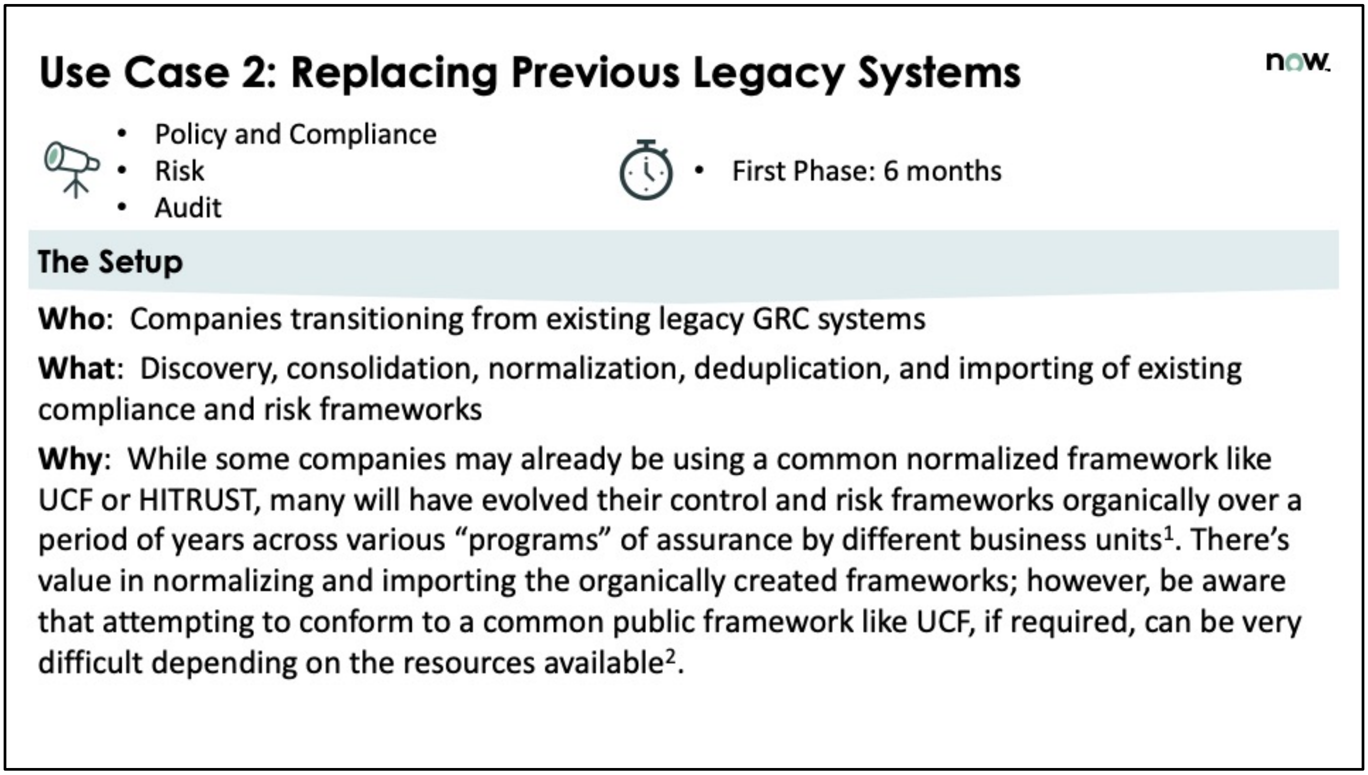
What we discovered about the company:

- Company is not yet public. Many key control owners were new to SOX and came from smaller DTC startups, while those familiar with the process had never used an automated platform for GRC (manual process spreadsheets).
- Very decentralized; compliance team had not previously used many other ServiceNow outside IT requests using the service catalog.
- Did not have discovery, service mapping stood up yet. IT had access to several different monitoring tools but nothing fully standardized
- Unique culture challenges – not everyone was happy about the upheaval from the re-organization and consolidation. Some were contractually obligated to stay on until a set time after the lockout period was reached. A few different stakeholders were swapped out while some of these challenges continued to shake out. Many stories from the backlog had to be cut from the MVP release to focus on IPO readiness with the goal to return for a second and third phase engagements post IPO.
- Focused on process first, then became more efficient in the ServiceNow GRC platform
- Audit Management team scoped based on entities and application depending on department

Configurations Summary:

- The following Entity Types were created: Business Application (relevant to IT Controls), Business Process and Department (relevant to business Controls)
- Business Applications were bulk loaded with plans to later relate these to business services discovered via Service Mapping
- Used manual Indicators (mechanism through which you can gather evidence) and Indicator Tasks (auto generated at various frequencies)
- Indicator drives workflow to send alerts, make changes, create a report, etc.
- Custom Indicator Task Workflow: Auto assignment rule to direct the Indicator Task
- Issue Management - one process and one form, different workflow stages based on the type (Control Test or Indicator Task)
- Event Management monitoring data and correlation for indicators and related configurations all pushed back to a future phase with the exception of a handful of critical systems where a specific kind of event

signaled immediate non-compliance and triggered a control issue along with a corresponding incident record.



Use Case 2: Replacing Previous Legacy Systems

- Policy and Compliance
- Risk
- Audit

- First Phase: 6 months

The Setup

Who: Companies transitioning from existing legacy GRC systems

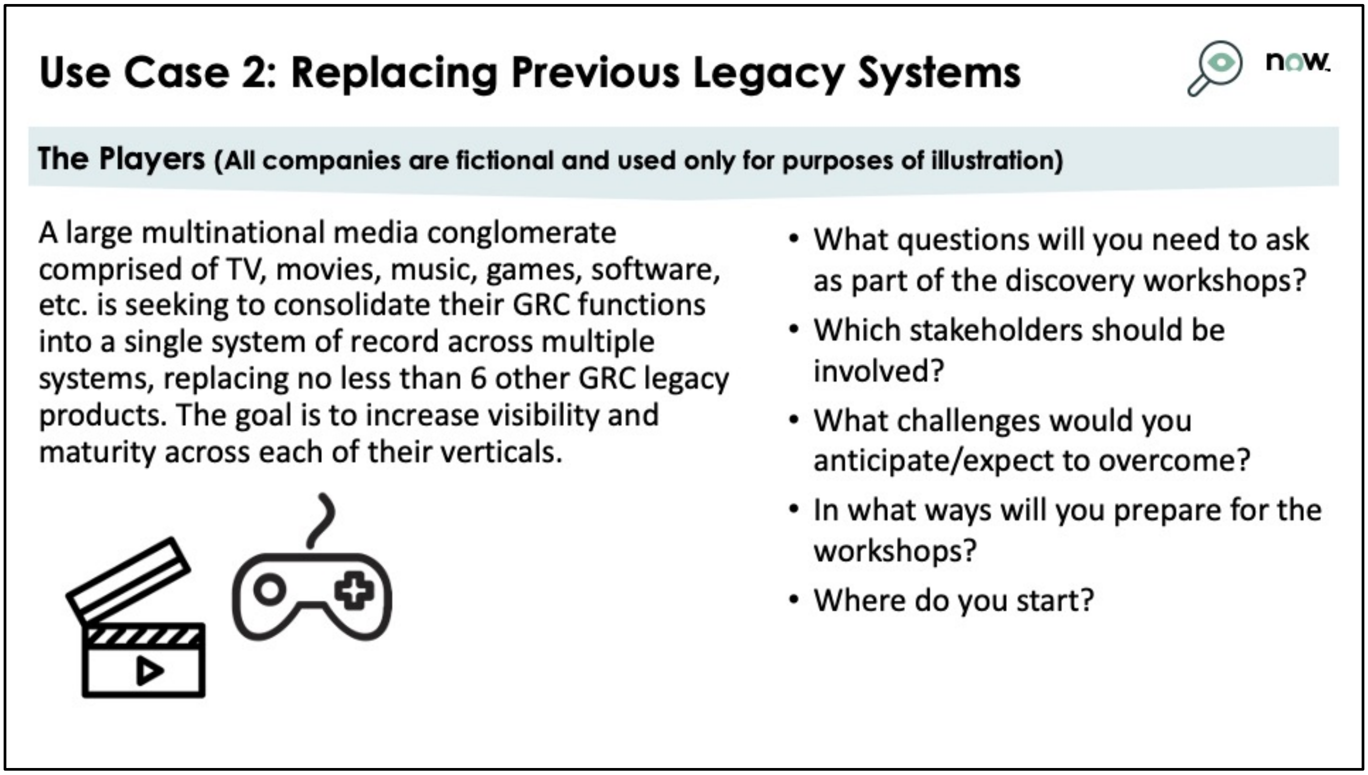
What: Discovery, consolidation, normalization, deduplication, and importing of existing compliance and risk frameworks

Why: While some companies may already be using a common normalized framework like UCF or HITRUST, many will have evolved their control and risk frameworks organically over a period of years across various “programs” of assurance by different business units[1]. There’s value in normalizing and importing the organically created frameworks; however, be aware that attempting to conform to a common public framework like UCF, if required, can be very difficult depending on the resources available[2].

[1] It is often the case that a department or business unit deploys a control after getting dinged by an auditor with a finding. Like a scar forming after a wound heals, organic control frameworks tend to focus on the specific outcomes to avoid specific operational pain. Sometimes it’s difficult to convince the control owner that their specific control is not unique and conforms to a common framework and taxonomy within the organization.

[2] While there are few newer tools and solutions to aid in this process such as the UCF’s own Mapper product (ucfmapper.com), control owners are understandably wary of setting their existing frameworks aside in favor of one developed outside of their environment. A lot of effort went into creating their existing controls. Control owners will often argue that their specific tests to ensure compliance are slightly different from system to system to satisfy different control objectives. In ServiceNow terminology, they are saying “the indicator” for these two systems is different, so the control objective must be different. In actuality, they are satisfying *the same control objective*. Overcoming their wariness of change is challenging.

When replicating this same discussion across dozens of control owners and potentially hundreds of controls, it becomes clear that the more expedient path is to focus on simply deduplicating, where possible, redundant controls within their own homegrown frameworks first and foremost. As this path is a significant step forward; adding the additional task of normalizing them against a completely new common framework increases scope and runs the risk of overrun with the project.



Use Case 2: Replacing Previous Legacy Systems

The Players (All companies are fictional and used only for purposes of illustration)

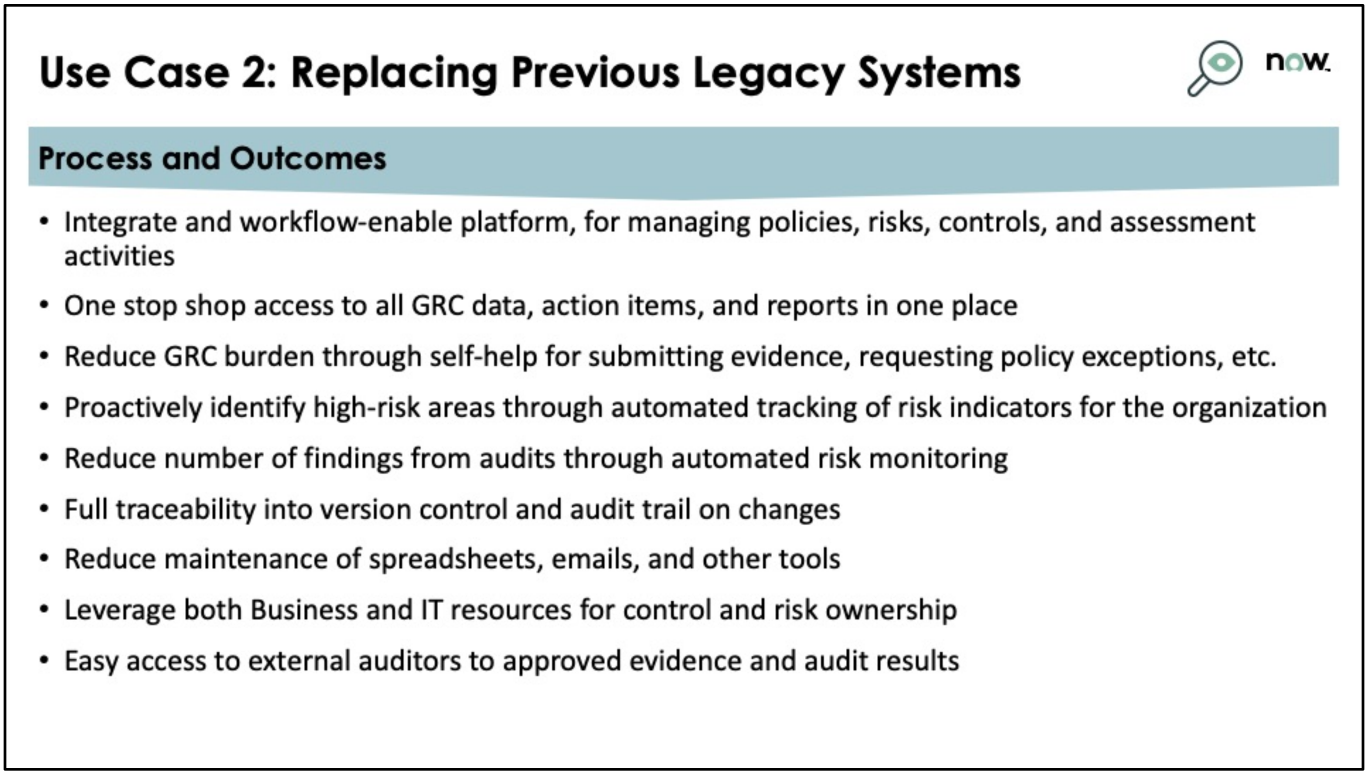
A large multinational media conglomerate comprised of TV, movies, music, games, software, etc. is seeking to consolidate their GRC functions into a single system of record across multiple systems, replacing no less than 6 other GRC legacy products. The goal is to increase visibility and maturity across each of their verticals.

- What questions will you need to ask as part of the discovery workshops?
- Which stakeholders should be involved?
- What challenges would you anticipate/expect to overcome?
- In what ways will you prepare for the workshops?
- Where do you start?

Scenario: Megatainment Corp, the parent umbrella company of several global media companies that design, develop, publish, and distribute media content, is in the first phase of a multi-year plan to re-structure it's organization. As a part of this restructuring, the board realizes that there is no simple way to visualize or understand the compliance status, audit readiness, or risk at the subsidiary company level, let alone at the enterprise level. Each company and vertical has implemented various systems and processes with little to no standardization across each silo. Obtaining unified reporting data currently involves as many as 6 different systems feeding data into a data warehouse and requires a dedicated team of Cognos analysts to build even the simplest of reports (already 2-4 months stale by the time that they are completed).

Megatainment does business across the globe and shares of both the parent company and several of its subsidiaries are traded on various exchanges throughout the world. Between the parent and subsidiaries, at least 8 different ServiceNow instances exist with varying levels of use and maturity. Each of the instances has been running the ITSM suite, with the oldest instance originally stood up on Fuji. While this task might seem daunting, the implementation team has secured executive sponsorship from the parent company CEO and each of the subsidiary company CEOs. In this initial phase, the goal is to transition the **game company** from their existing GRC legacy product, in use since 2011, while helping to create a model for each of the other companies to follow. The game company's data will be brought into a new central instance. The goal to create a model for managing compliance and risk at the parent company level with insight into the compliance status of subsidiaries and risk levels of various development projects during their various product lifecycles. For the game company, this will involve tracking project data from ORACLE Netsuite OpenAir (Project Management) and existing asset and CI data tracked in the platform currently via Discovery, Service Mapping, and Event Management.

Megatainment wants to see tangible high-level reporting progress at the centralized level within six months of kicking off this effort.



Use Case 2: Replacing Previous Legacy Systems

Process and Outcomes

- Integrate and workflow-enable platform, for managing policies, risks, controls, and assessment activities
- One stop shop access to all GRC data, action items, and reports in one place
- Reduce GRC burden through self-help for submitting evidence, requesting policy exceptions, etc.
- Proactively identify high-risk areas through automated tracking of risk indicators for the organization
- Reduce number of findings from audits through automated risk monitoring
- Full traceability into version control and audit trail on changes
- Reduce maintenance of spreadsheets, emails, and other tools
- Leverage both Business and IT resources for control and risk ownership
- Easy access to external auditors to approved evidence and audit results

What was discovered:

- Various concerns about GDPR, data sovereignty, and security made the proposition of a single "Instance to Rule Them All" a non-starter and a federated model was immediately adopted as the path forward with the understanding that some of the many instances used by various groups may be subject to deduplication efforts in the future (the Movie company had 3 in the US region alone for example) and those efforts would likely be able to start once the initial pilot phase had completed
- Focus and emphasis on maintaining baseline instances where possible and each customization was weighed against estimated technical debt required to test and maintain into the future
- 400 Stories (requirements) and 400 test cases
- Regulations/Frameworks: NIST, SOX and PCI to start
- Started with a focus on Risk (complexity of the Risk model)
- Customer made many decisions, only to later change their minds
- Data (Policies, Controls, Risks, etc.) took a significant amount of time
- Lack of understanding of process and GRC functionality can cause additional, unnecessary customization
- Multi-language email notifications; hard to agree on when they should occur and what they should contain

Configurations Summary:

- Initial phase resulted in unidirectional instance data binding between game and centralized instance.
- Leveraged Common Services Data Model and CMDB for many of the entity types required
- Integrated OpenAir project status data and populated the pm_project and cmdb_ci_business_application tables at the top line level to allow for different entity types to be created based on project life cycle, with Risk Frameworks applied for entities in development, production, and end of life, as well as entities identified as "AAA" (designation based on projected budget of $100 million or more and/or projected revenues exceeding $250 million).
- Multi-tier review and approval
- Configured Controls
- Adjusted flows to move attestation completion
- Built a custom Risk scoring model as the baseline scoring model was not sufficient