

## Agenda

**Members Attending:** Blanchard, Cromer, Frey, Kirmse (Chair), Lander, Robinson, Sallot

**Others Attending:** A. Baumstein, C. Benjamin, Patrick Connelly, W. Curry, Adam Heward, D. Huelsman, J. Madey, I. Moffat, A. Singh-Kreitz, Alvin Woodbury

**3:00 to 4:00 pm**

**1/28/2014**

**CSE 507**

### 1. Membership Update

**Kris Kirmse**

- Lane Blanchard has replaced Tom Livoti as representative from Health Sciences Center
- Chair reminds those in attendance that 'voting' is restricted to appointed committee members; Blanchard, Cromer, Frey, Kirmse (Tie-breaker only) Lander, Olson, Robinson, Sallot, Yeffet (student representative). There is currently no faculty representative.

### 2. ITSM Review & Recommendation

**Ayola Singh-Kreitz**

*Refer to 69248-ITSM Tool Recommendation for SIAC 1-24-2014 v2.pptx, distributed to members in advance.*

- Ayola: The Tool Evaluation Team solicited cross-campus input re: tool selection;
  - reviewed multiple companies;
  - short-listed 5;
  - top 3 were BMC, ServiceNow, Cherwell;
  - Top 2 were ServiceNow & Cherwell; These were the names passed to the ITSM Steering Committee;
  - The ITSM Steering Committee selected Cherwell
    - Price was a significant factor in the final decision; Cherwell is less than ½ the cost of ServiceNow
- The Steering Committee's selection is now coming to SIAC for endorsement. SIAC members polled on question of whether to endorse Steering Committee's choice:
  - Yes: 4
  - No: 0
  - Abstain: 3
- Ayola also announced Richard Lowery as new UF Computing Help Desk Manager, succeeding her, as she is moving to the new position of ITSM Delivery Manager.

### 3. CNS: Network Services and Enterprise Infrastructure & Operations **Iain Moffat**

- CNS is being split into two units:

# IT Governance: Shared IT Infrastructure Advisory Committee (SIAC)



- a computing/storage/datacenter organization: Enterprise Infrastructure & Operations (EI&O), with Chris Easley as Interim Director
- a network service organization, yet to be officially named, headed by Tom Livoti
- The EI&O organization will merge two existing groups (Enterprise Systems Infrastructure, and Open Systems) into a combined “Computing Infrastructure and Systems Administration” group within EI&O
- Change Drivers: Why make these changes? The reorganized EI&O is being structured so as to provide improved focus in several areas:
  - More customer-focused & Responsive
  - Push work to the most appropriate level, so that most-skilled tech staff don’t have their time consumed with minor issues that can be handled in a more routine fashion:
    - 3 tiers:
      - Tier 1: End-user Support & Data Center Operations
      - Tier 2, Day-to-day System Administration
      - Tier 3; Strategic Planning, Architecture, & Design
  - More highly-available; i.e. Linux, Windows, and Core Infrastructure groups will be larger (more people), to better ensure full coverage
  - More commoditization; more automation, more self-service
  - Innovation: allowing most-skilled staff to spend more time doing innovative work
  - People; making sure we have growth-path for people, both technically and/or managerially
  - Better teamwork; de-siloizing and focus on Services, across EI&O
  - Staff retention: Allowing the more-skilled staff to focus on things that are interesting & challenging to them, instead of being bogged down in day-to-day ‘little stuff’
  - Better integration with ITSM, holistically across the organization
  - Clearer focus on Project Portfolio Management (PPM) so that projects are scheduled and resources allocated in a coherent fashion organization-wide

## 4. Office365/SkyDrive

Iain Moffat

- Now called OneDrive (MS lost lawsuit over the name ‘SkyDrive’); so maybe expect to see: “GatorBox Powered by OneDrive”
- Still on target for Early March to have infrastructure ready; still need to discuss/coordinate the ‘on-boarding’ process. There may be a limited pilot first, before general availability.
- Access to Office Web-Apps expected in the same time-frame (March)
- This will be open to Students, Faculty, and Staff who are eligible (i.e., can certify that they don’t deal with Personal Health Information [PHI])

## 5. Email Storage

Iain Moffat

# IT Governance: Shared IT Infrastructure Advisory Committee (SIAC)



- Currently mail is automatic deletion from Exchange after 1 year, but there are 3-year retention policies
- Moffat thinks CISO Rob Adams is discussing this issue with UF General Counsel
- Office365 has unlimited time, but total storage limit (25GB)
- Exchange 2013 is being designed for 25GB per user; coming probably May. In general, EI&O is trying to architect the Exchange 2013 deployment to mirror Office365

## 6. Remote Access Policy

Avi Baumstein

- New Policy: Draft has been recommended by ISCAC
- Key item is definition of “Remote Access” – taken from NIST 800-53 (“Recommended Security Controls for Federal Information Systems and Organizations”); any access over a connection not controlled by the University.
- Note in the Standard: Approved Remote Access Methods are to be registered in Net Services Database; this may change if they find/create a more appropriate home for these registrations
- Web-servers that are registered with Net Services will be considered approved.
- VPN is an approved method which does not “cross a boundary.”
- Goal is to get everything on VPN; then block unapproved connections (someday)
- Benjamin: What about Housing’s VPN? AB: It will need to be reviewed for approval
- Draft may be shared with others for feedback
- This will be a topic at the next Campus IT Directors’ Meeting (2/20/2014); please provide feedback before then.
- Cromer: Supports concept, but needs more details/specifics
- Lander: What about Lync federation? You can share desktops, files, etc. AB: That will probably be considered “Remote Access”
- Webex? Probably falls into “Remote Access”
- InfoSec may write provision that this policy applies to externally-initiated connections, and have Separate guidelines for internally-initiated connections.
- Send Avi Feedback before 2/20/14

## 7. Infrastructure Applications Advisory Committee (standing item)

Eric Olson

Cancelled last month/Eric not present

## 8. Other Topics?

All

- Shibboleth IdP Code Update: Warren Curry; this has been load-testing; Announcement emails will be going out shortly

## 9. Isilon – General Discussion

All

- Robinson: User Experience?

# IT Governance: Shared IT Infrastructure Advisory Committee (SIAC)



- Sallot: Mostly stable during fall, but got a little flaky in Dec.
- Moffat: There was memory leak in SMB service; putting in patch ASAP
- Sallot: Suggested Isilon User Group/list

## 10. General Counsel Policy on Email Forwarding – General Discussion All

- Cromer (from email): “I'd like to add discussion of the new policy prohibiting forwarding of UF Business email. This puts many UF/IFAS Extension agents in a quandary, as they work in counties where the county government requires them to use the county email system. We also have courtesy faculty who work for USDA and FAMU, among others. They need GatorLink credentials to access UF resources, but want to forward their email to their primary system.”
- Kirmse: As written, the policy forbids forwarding from UF GatorLink (“Webmail”) to UF Exchange
- Not everyone who gets a GatorLink id is eligible for a UF mailbox
- Courtesy faculty from other agencies, and extension agents are problematic cases
- W. Curry: This policy will be enforced based on affiliations. Affiliations are being/have been refined to provide ability to treat groups appropriately.

**11. Next Meeting** – the 4<sup>th</sup> Tuesday from 3:00pm to 4:00pm – Feb 25th in CSE 507

## Additional Information:

- UF IT Governance Home: <http://www.it.ufl.edu/governance/>
- Shared Infrastructure Advisory Committee (SIAC) website: <https://connect.ufl.edu/it/SIAC/>



# IT Service Management

Tool Evaluation Recommendation

January 2014

# Table of Contents

- ▶ Executive Summary
- ▶ Background and Evaluation Participants
- ▶ ITSM Tool Evaluation Approach
- ▶ Results and Recommendation
  
- ▶ Appendix: Supporting Material

# Executive Summary

- ▶ The ITSM Tool Evaluation Team has completed its analysis under the guidance of the ITSM Steering Committee
- ▶ The recommendation is to select Cherwell as the next generation ITSM toolset.
- ▶ This summary packet contains background information and summary analysis reference material.

# Background

- ▶ This recommendation is for the selection of a vendor for an integrated IT Service Management (ITSM) software solution.
- ▶ This solution automates end-to-end workflow for supporting IT end users and managing IT services and provides a full suite of applications for use by IT help desk and technical teams across UF.
- ▶ This tool will provide the ability for IT teams and shared services teams across UF to collaborate, report, and measure the delivery of IT services.



# ITSM Tool Evaluation Participants

- ▶ In August 2013, the ITSM Tool Evaluation team was formed under the guidance of the ITSM Steering Committee.
- ▶ Facilitation and support for the evaluation team was provided by Purchasing Coordinator Rob Luetjen and Gartner.

## **ITSM Steering Committee:**

Rob Adams\*  
Al Amirin  
Dan Cromer  
Margaret Fields  
David Gruber  
Michael McKee  
Kris Kirmse  
Fedro Zazueta

*\* Chair*

## **ITSM Tool Evaluation Team:**

Elizabeth Amdur  
Chris Easley  
Jim Freymann\*  
Shane Massey  
Christina Neipert  
Barb Sedesse  
Ayola Singh-Kreitz\*

*\* Chairs*

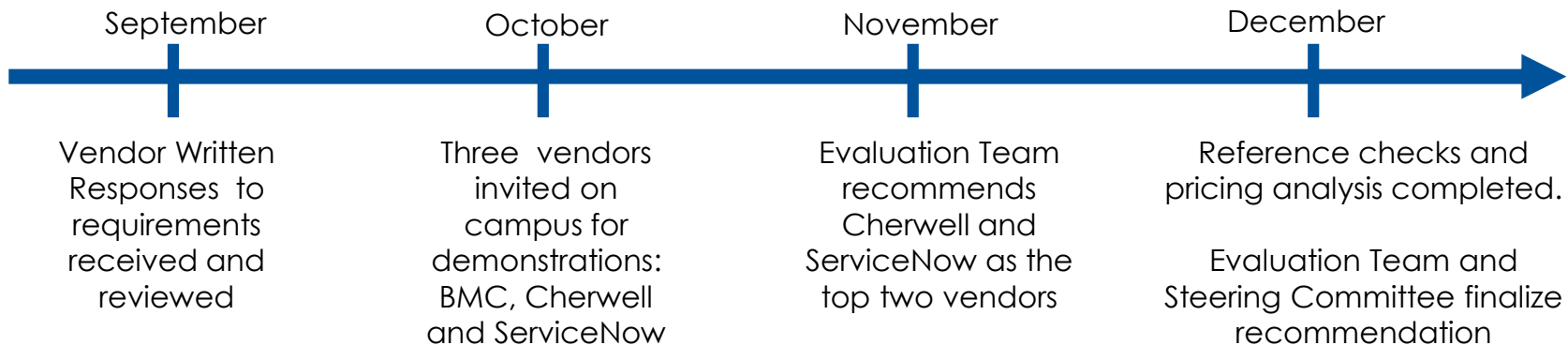
# ITSM Tool Evaluation Approach

- ▶ The tool evaluation process included written responses, onsite demonstrations, reference checks and pricing analysis.

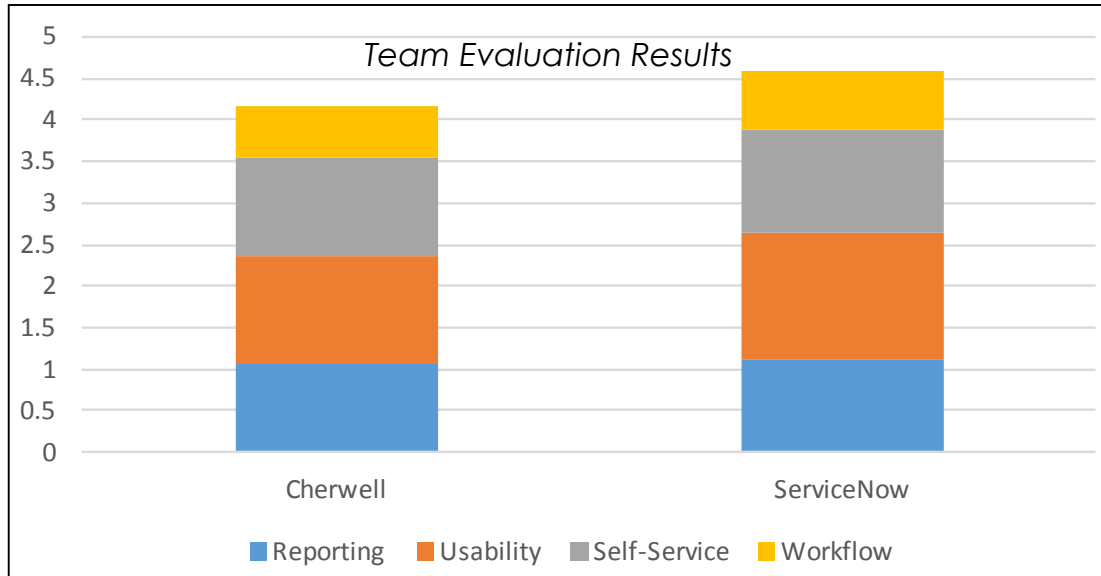
## ITSM Vendors who Responded:

BMC  
Cherwell  
IBM  
HP  
LANDesk  
ServiceNow

## ITSM Tool Recommendation Timeline



# Results and Recommendation



- ▶ The Evaluation Team is confident both tools can meet UF needs
  - ServiceNow ranked slightly higher in functionality
  - ServiceNow was more than twice the price of Cherwell and has a significantly more complex cost model

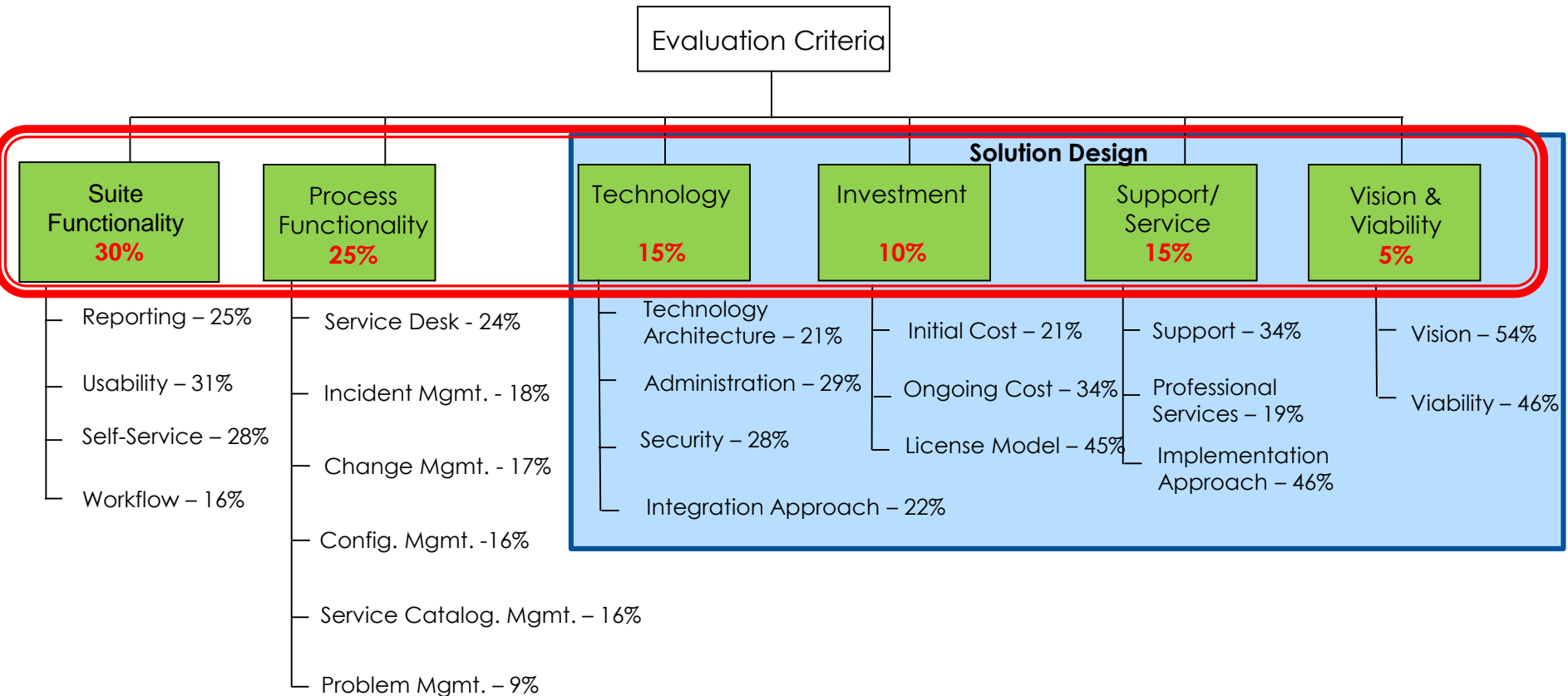
▶ With guidance and concurrence from the ITSM Steering Committee, the recommendation is to select **Cherwell** for the next generation ITSM solution.

# Appendix

# ITSM Tool Evaluation Vendors

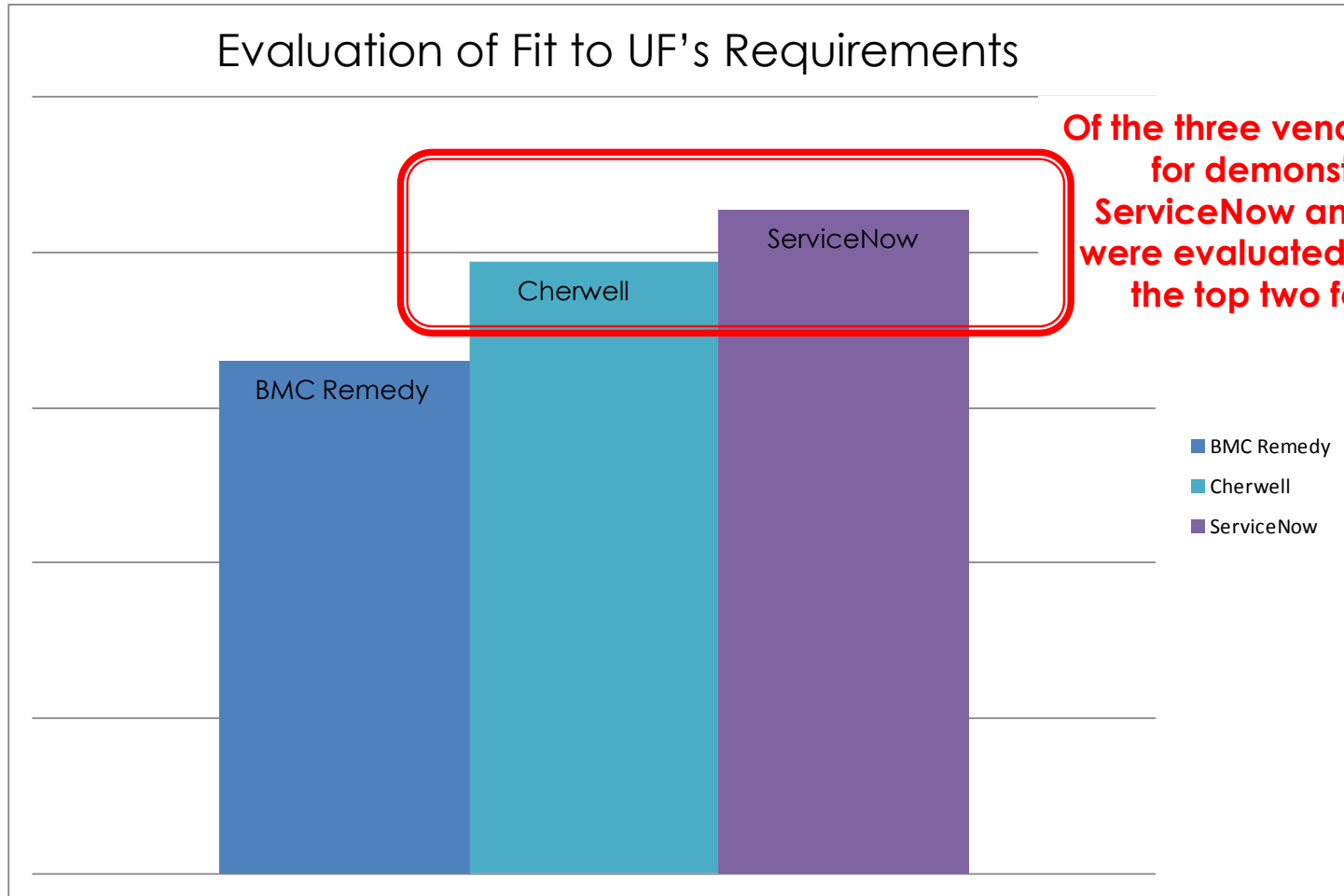
- ▶ Vendors Selected to Provide Information Based On:
  - Research by UF Purchasing
  - Task Force interviews with other Universities and information on top short-listed ITSM vendors
  - Gartner Magic Quadrant criteria, including:
    - The vendor must have at least \$10 million in annual revenue derived from ITSM products.
    - The vendor must have functionality to support a specific set of ITSM processes.
    - The vendor must provide 10 qualifying customer references meeting the following criteria:
      - The customer must be utilizing more than 100 concurrent licenses or 300 named licenses.
      - References must include examples of both licensing models: on-premise and off-premise (e.g., SaaS).
      - References must be located in at least three of the following regions: North America, South America, Europe, Middle East, Africa, Asia and Australia.

# ITSM Tool Evaluation Weightings



- ▶ The Tool Evaluation Team met and agreed upon the relative evaluation criteria weightings shown above. These weightings were reviewed and accepted by the ITSM Steering Committee.

# ITSM Tool Evaluation Summary



Of the three vendors selected for demonstrations, ServiceNow and Cherwell were evaluated by team as the top two for best fit

# Key Trade-offs Noted by Evaluation Team



## Evaluation Criteria

## ServiceNow

## Cherwell

Suite & Process  
Functionality

- Evaluated as a slightly better fit for usability, reporting, and process capabilities

- Strong offering but not as robust as ServiceNow

Technical  
Architecture

- Only available as a SaaS model
- Single platform and simple architecture

- Available as SaaS or On-Premise model with ability to switch between models
- Web and desktop client

Service and  
Support

- More support services and community of resources

- Less established network of community resources

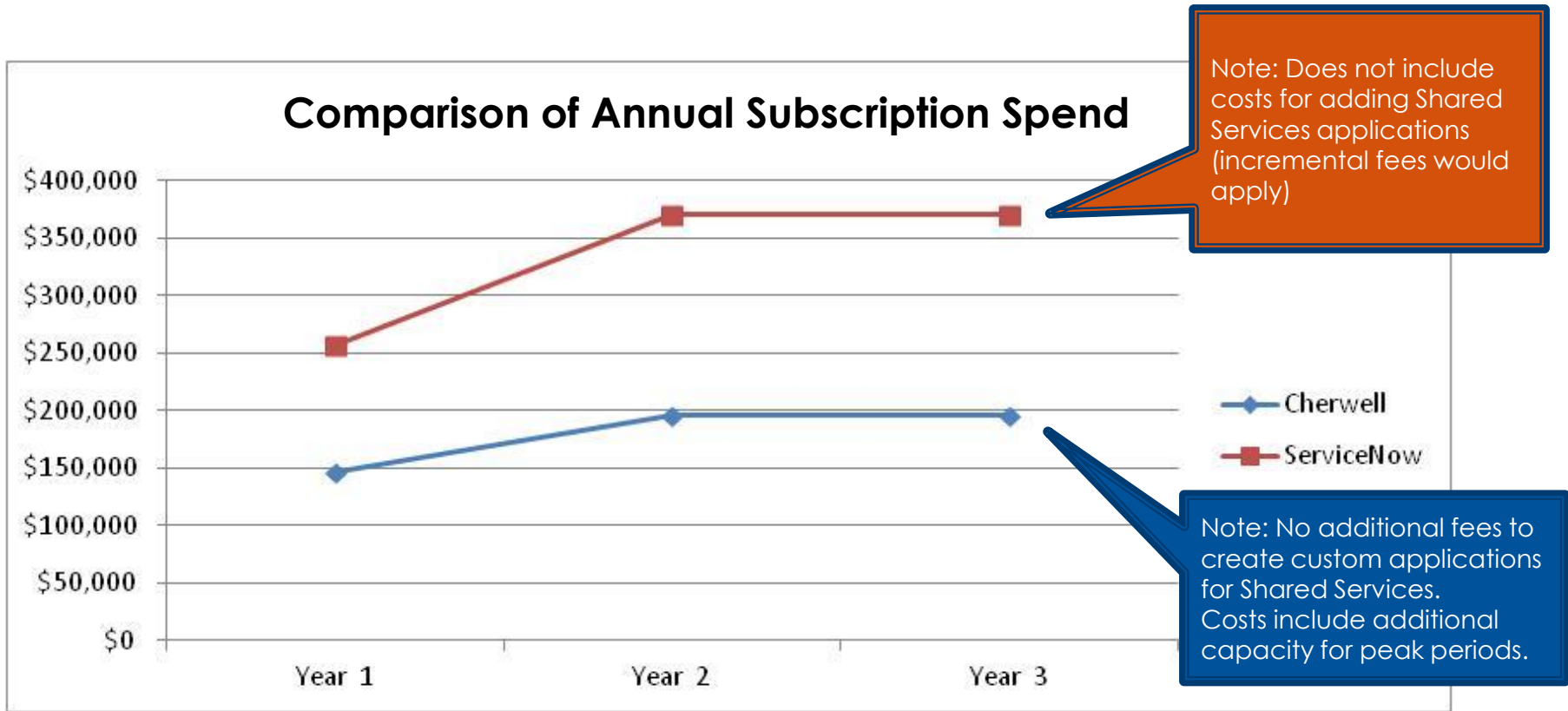
Cost

- More complicated pricing / licensing model and significantly more expensive overall
- Incremental costs for additional applications and Shared Services usage

- Simple pricing model and less expensive overall
- No additional cost for adding applications for Shared Services



# Pricing Analysis



- ▶ Note: The ramp up in pricing for both vendors reflects additional IT Partners onboarding after UFIT

---

## Purpose:

The purpose of this policy is to define how the University of Florida controls remote access to university information systems and networks in order to prevent unauthorized use.

---

## Scope:

This policy applies to all methods the university implements to allow remote access to its services, information systems and networks.

---

## Policy:

1. All methods the university provides to offer remote access to services and information systems must be assessed for security, approved, documented and controlled. The university will allow external network access only to approved remote access end points.
2. Remote access methods must employ appropriate security technologies to secure the session, as well as prevent unauthorized usage.

---

## Responsibilities:

1. All members of the University of Florida Constituency are responsible for protecting remote access methods, devices and credentials assigned to them. Users are responsible for maintaining the security of computers and devices used to remotely access university resources.
2. Information Security Managers (ISMs) are responsible for documenting and implementing controls for all remote access methods implemented within their unit. ISMs are also responsible for monitoring of unit-implemented remote access methods for unauthorized use, and taking appropriate action upon discovery of unauthorized use, including notification of the UF Information Security Incident Response Team.
3. The Vice President and Chief Information Officer (CIO) is responsible for approval of remote access methods and resources.

---

Policy Number:  
SEC-TS-nnn

Policy Family:  
Information Security

Category:  
Technical Security

Effective Date:  
xx/xx/201x

## Policy: Remote Access



4. The Vice President and Chief Information Officer (CIO) is responsible for implementing systems and specifications to facilitate unit compliance with this policy.

---

### Authority:

UF-1.0102: Policies on Information Technology and Security

---

### References:

NIST 800-53 v3: AC-17, AC-17 enh 2

DRAFT

---

Policy Number:	Policy Family:	Category:	Effective Date:
SEC-TS-nnn	Information Security	Technical Security	xx/xx/201x

---

## **Purpose:**

To establish usage and documentation requirements for remote access methods used at the University of Florida.

---

## **Standard:**

1. Firewalls and other technology will be used to restrict Remote Access to only approved Remote Access mechanisms.
2. Approved remote access mechanisms will be registered in the Net Services Database.
3. Web servers that provide service to the public, and do not store or provide access to Restricted Data are approved methods of remote access once registered in the Net Services Database.
4. To be approved, Remote Access mechanisms must include the following technical capabilities:
  - a. Allow only identified, authenticated and authorized users to connect.
  - b. Provide for strong encryption of traffic.
  - c. Audit logs contain sufficient information to establish the following:
    - i. Event type (authentication, connection or disconnection)
    - ii. Date and time
    - iii. User associated with the event
    - iv. Remote and local IP addresses
    - v. Event success or failure
5. Interconnections to the UF Network require interconnection agreements. Access must be restricted to the minimum necessary to achieve the goals of the interconnection.

## Standard: Remote Access



6. Documentation of remote access mechanisms includes:
  - a. Local and remote end points, and mechanisms intended to enforce connection only by intended end points.
  - b. Intended users (based upon role or group) and mechanisms to enforce those restrictions.
  - c. What university information systems and data remote users may access, and methods to enforce those restrictions.
  - d. Guidance provided to users of appropriate uses of the remote access method.
7. Remote access methods must be monitored for unauthorized use, and signs of unauthorized use promptly reported.

---

### References:

---

Standard Number: SEC-TS- <del>nnn</del> .nn	Standard Family: Information Security	Category: Technical Security	Effective Date: xx/xx/201x
--	--	---------------------------------	-------------------------------