HEALTH
SCIENCES
CHIEF INFORMATION
OFFICE

SEPTEMBER UNIT REPORTS

NM OFFICE OF MEDICAL INVESTIGATOR-**MARTIN WETTERSTROM**

APPLICATIONS-**RAY AVILA**

SYSTEMS-**PHIL MARQUEZ**

SECURITY-**MIKE MEYER**

TECHNOLOGY SUPPORT-**RICK ADCOCK**

UH IT NETWORK/NETSEC-**CHARLIE WEAVER**

HSC 2021 VISION

NEW MEXICO OFFICE OF THE MEDICAL INVESTIGATOR

MARTIN WETTERSTROM

Accomplishments

- New Case Management System (CMS)
  - Live on August 10th
  - Replaced two separate legacy CMS systems
  - Retiring out of support server operating systems
  - Developed change management tracking in SharePoint
  - For transparency weekly newsletter and access to SharePoint for end users
- VPN Appliance
  - Retired OMI in house VPN appliance
  - Remaining needed VPN access using pulse
- Reports and Dashboards
  - Automated daily/weekly/monthly reports
  - Dashboards tracking daily/monthly numbers
  - No more manual data pulls for KPI tracking

In-Progress

- CMS
  - Continued application improvements
  - Process improvement
  - Integration with NMBVS
  - Integration with labs
- Compliance
  - Windows 7 elimination, 1 remaining
  - Retire legacy CMS servers
  - Replace legacy access points
  - Windows 10 servicing versions

Metrics

- CMS
  - Total change request to date 78
  - Completed change requests to date 4
- Compliance
  - 19H1 one remaining
  - 19H2 two remaining
  - Windows 7 one remaining

Recognition

- Michael Garcia and Marc Leasure for their continued dedication to client satisfaction and providing excellent service. Marc Leasure for receiving the HSC CIO IT Rockstar award.

HSC APPLICATIONS TEAM

RAY AVILA

Accomplishments

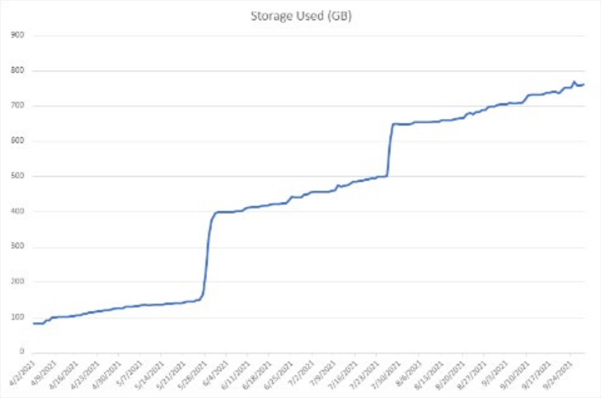
- Developed HSC 184, “Fluoroscopy Refresher Training” course (urgent) in preparation for JHACO
    - for Reed G Selwyn, Regents’ Professor & Chief, Diagnostic Medical Physics, Department of Radiology
- Conducted Learning Central Admin Training
- HSC Moodle Administration and Support
    - Bulk user uploads and password resets
    - Enrollments
    - Issued Certificates
- Policy Manager Administration
    - implemented UNMMG Department/Group member automation for attestation
    - Resolved Multiple PowerUser selection issue
- Zoom Administration
    - Resolved Telehealth display name and department
- SOM support
    - Compiled data for 2021 HSC Databook
    - Queries, reports, and application modification requests
- Upgraded TOPAZ application in development

In-Progress

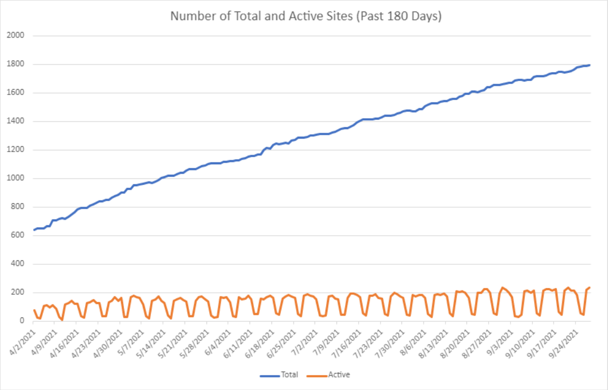
- M365 – Target date 3/31/2022
    - Consultations
    - SharePoint 2010 to SharePoint Online migrations and conversions
    - HSC CIO Office projects in Planner
    - User Group and instructional resources development
- Faculty Directory – Target date 10/11/2021
    - Deployed automated file creation process for website content
    - Testing/final file generation modifications

Metrics

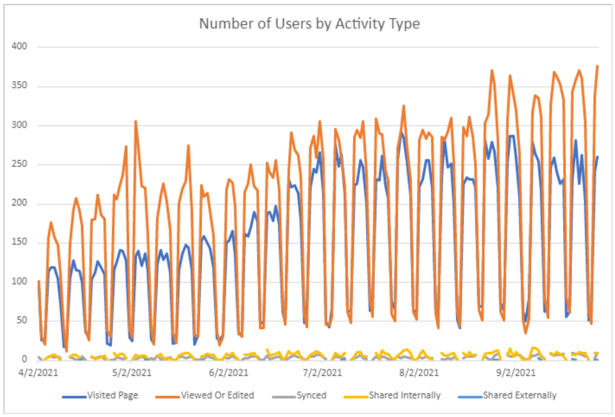
- SharePoint usage
    - 180 Day SharePoint Storage Trend



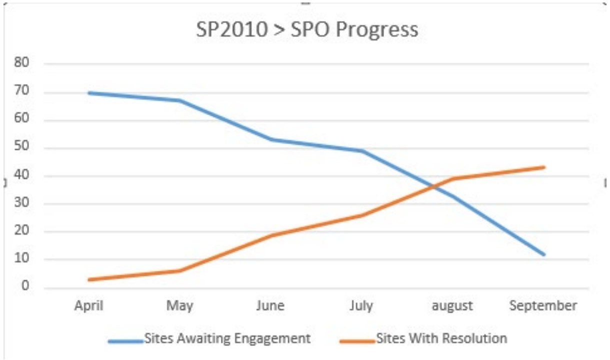
- 180 Day SharePoint Site Count



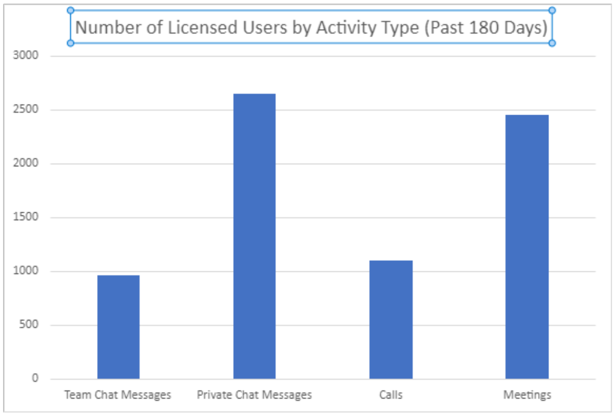
- 180 Day SharePoint User Activity



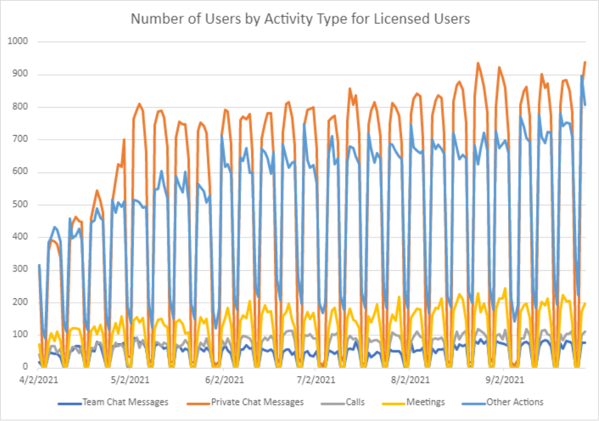
- Legacy SharePoint to m365 migration



- M365 Teams
  - 180 Day Teams Component Usage



- 180 Day Teams User Activity



Recognition

- Lewis Worley for his having stepped into an operational guidance role for the HSC Applications Team during my absence this past month. He was able to monitor and keep the team on track for continued efficient operations.

HSC SYSTEMS TEAM

PHIL MARQUEZ

Accomplishments

- No new major projects in September
- Metallic cloud backup
  - Working to identify servers and systems not previously backed up to gauge the scale of unprotected data across the organization
  - Continuing roadshow on Metallic capabilities, benefits, and costs
- Supported Security implementations
  - Provided support for implementation of new Phishing Reporter button and removal of old
  - Provided support for implementation of BYOD with device registration configuration
  - Completed inventory to ensure Carbon Black installed everywhere
- Azure/M365
  - Old Exchange environment decommissioned and the supporting Active Directory domain removed

In-Progress

- Azure/M365
  - Continue working with UNMH to support testing and implementation of Azure MFA
- On-site storage replacement
  - Continued working with vendors to replace on premise storage solutions that are unreliable and nearing end of support. We will plan to replace half our storage this year and the rest next year
- Nutanix Hyper-converged environment capacity
  - In the process of increasing memory across all nodes in our virtual host environment to support ongoing creation and operation of virtual servers across the organization. This will get us through this year, but will need to add additional nodes into the cluster by next year
  - Currently, updating firmware and OS across the cluster in preparation for memory upgrade. Rolling upgrades with no impact expected

Metrics

- 100% system uptime

Recognition

- Judson Carter for keeping the lights on. Judson basically has his hands in almost all of CIO Systems operations…in a good way! Thanks for his ongoing attention to detail and constantly striving for excellence.

INFORMATION SECURITY OFFICE

MIKE MEYER

Accomplishments

- Completed security review and risk assessment for use of PHI on Microsoft 365
  - Determined that about 30% (6000+) accounts have not registered devices for multi-factor authentication (MFA) because they only work on campus, where MFA is not required
  - This is an exploitable vulnerability that we need to address before allowing PHI
  - ISO working with IT to formulate a path forward to facilitate device registration by all users
  - ISO will issue risk assessment, security plan and related documentation once this vulnerability is addressed
- Improved security posture of MFA, EDR and perimeter vulnerability reduction impeded CLA during its annual independent penetration testing
  - CLA was not able to compromise 365 accounts primarily due to multi-factor authentication
  - Carbon Black endpoint detection and response (EDR) alerted and blocked many (but not all) lateral moves and privilege escalations during internal penetration testing
  - With one exception (Pulse VPN), "pentesters" were not able to find exploitable vulnerabilities on publicly accessible systems
- Implemented single solution (Microsoft) MFA for 365, VPN, Citrix Access Gateway (CAG)
  - Microsoft 365 implementation completed in Aug
  - VPN transition to Microsoft MFA completed in Sep
  - CAG still in progress, but most technical challenges have been addressed

In-Progress

- Improve vulnerability management
  - Conduct full-scale discovery scan to characterize devices on the network
  - Obtain approval of the vulnerability management policy and plan
  - Standardize on a common set of scanning tools and procedures

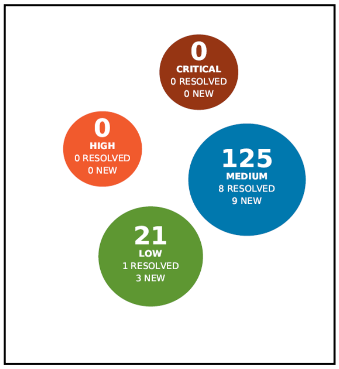
- Develop and publish a roadmap for implementing the "Top Ten Security Enhancements"
  - MFA and EDR complete
  - Currently researching data loss prevention options and roadmap
- Develop ransomware "playbook" for incident response
  - Increase speed of response
  - Provide a framework for incident response training
- Resume phishing simulations this year
  - NLT November, possibly Oct
  - Developing learning strategies now

Metrics

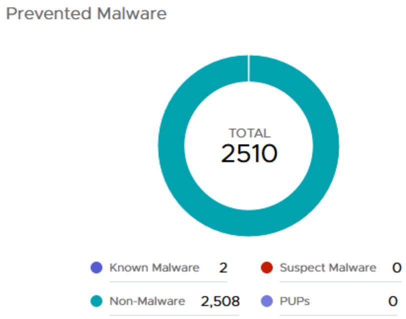
• Change Requests:	8
• SSL Certificate Requests:	6
• Data Transfer Assistance (DUA/SFTP):	21
• Security Reviews for Technology Purchases:	22

- Vulnerability Scans: 18
- Other Requests for Support: 48
- Perimeter Vulnerabilities:
    - Critical: 0
    - High: 0
    - Medium 123 (Increase of 2)

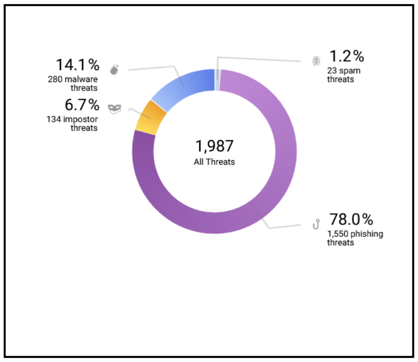
Perimeter Vulnerabilities



Malware Prevented by Endpoint Detection and Recovery (EDR)



Taxonomy of Incoming Email Threats Blocked by Proofpoint



TECHNOLOGY SUPPORT

RICK ADCOCK

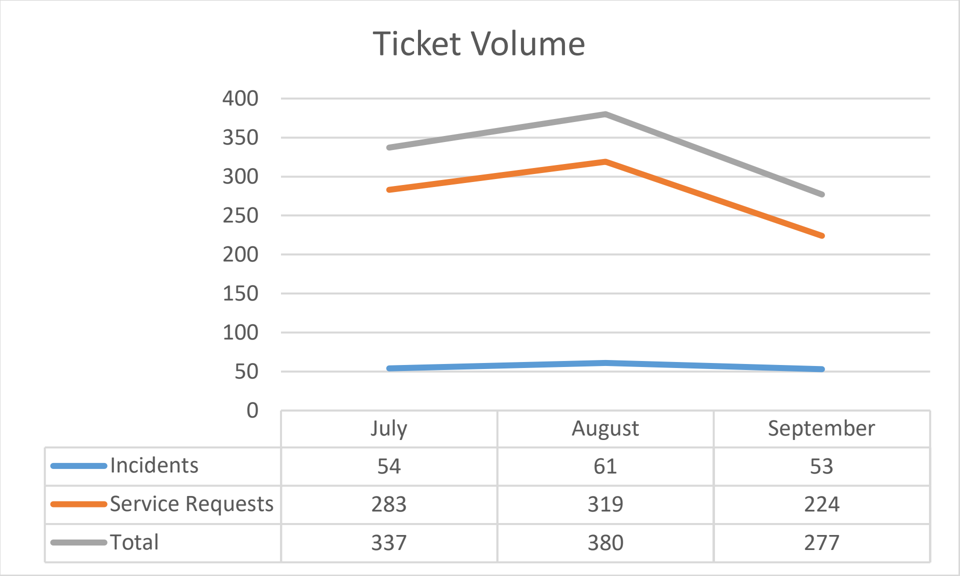
Accomplishments

- Assist employees with the change of the VPN MFA from DUO to Azure
  - Developed schedule and data set for the transition
  - Executed the change in requirements according to the schedule
  - Provided IT end user support
  - Monitored and reported progress
- Created the next Windows 10 Gold Image (new version of Windows 10 and removing McAfee antivirus/encryption)
  - Acquired the UNM Windows 10 H2 (new) version of Windows 10
  - Updated software and patches
  - Image has been checked for quality control
  - Released for Testing
- Re-deployed student computing workstations in HSLIC to the third and fourth floors
  - Update several workstations with wireless cards to be deployed where no physical ethernet exists
  - Purchased new monitors for workstation to be deployed in cubicles
  - Installed the workstations and the third and fourth floors of HSLIC

In-Progress

- Moving affiliate accounts the HSC VPN in order to demise the affiliate VPN
  - Analyze data set to determine affected affiliate accounts
  - Target communications and instructions to affected accounts to move VPN connections
  - Demise the affiliate VPN connection
- Moving additional HSC employees O365 licensing from main campus O365 to HSC O365
  - Created two groups of target email to be sent to affected accounts
  - Emails have been sent
  - First cutover is 10/4, and the second cutover is 10/18
- Testing the workstation hardening group policy of the Department of Pathology
  - Previously tested on workstations in the CIO organizations
  - Deployed to workstations in the Department of Pathology
  - Will target larger departments for more testing
  - Will deploy to the rest of the HSC workstations
- Assisting with moving health system workstations encryption key escrow from McAfee to Active Directory
  - Developing and testing script to move the escrow
- Assisting with the Office of University Counsel move from Time Matters application to HighQ Collaborative Instance
  - Assisted with vendor access

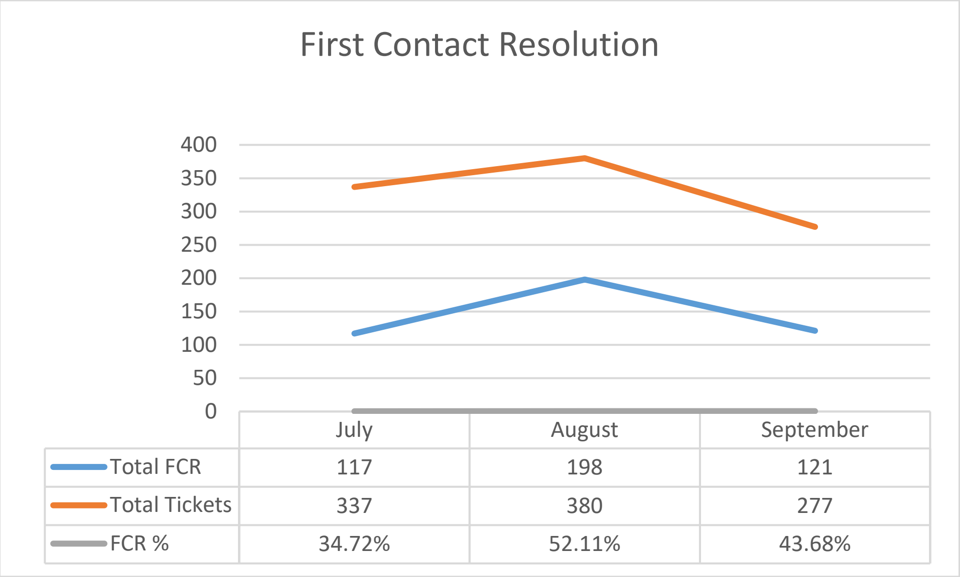
Metrics


Ticket Volume

	July	August	September
Incidents	54	61	53
Service Requests	283	319	224
Total	337	380	277

Automated Call Distribution Data

	July	August	September
Call Volume	1739	1764	1764
Avg. Speed to Answer	3:33	2:57	1:45
Abandon Call Rate	14.84%	12.70%	7.48%


First Contact Resolution

	July	August	September
Total FCR	117	198	121
Total Tickets	337	380	277
FCR %	34.72%	52.11%	43.68%

Recognition

- Scott Hanson – Scott has been instrumental in many things across the enterprise. He has worked through several projects with my teams, but I do want to acknowledge that Scott works for the "Enterprise" and has been an excellent example of the attitude and work ethic needed for the entire IT community.

UH IT NETWORK/NETSEC

CHARLIE WEAVER

Accomplishments

- Distribution switch replacements continuing
    - Hospital locations on hold due to ongoing JHACO & CMS presence
    - HSC locations in process
    - 12 HSC buildings completed/7 remaining
    - Anticipate completion before the end of the year
- Core switch model selection completed
    - Will look for additional funds
- Assisted Cyber team in compiling CLA data
- Multiple JNIS sub-team activities (Incident Management, Vulnerability Management, etc.) in flight
- CAG MFA integration testing completed
    - Rollout timeframe TBD

In-Progress

- Network Managed Service option being explored
    - Planning for RFP
- FY22 equipment purchases beginning due to six+ month supply chain related lead-times
- UH distribution switch replacement on hold due to JHACO/CMS activities
    - Will resume end of month
- OMI Wireless AP replacement in planning stages
- MDC / BBRP data center network modifications in planning stage
    - 10/16 implementation

Metrics

Total Access Layer Switches (UNMH, HSC, Remote):	~700
Total Access Layer Switches replaced to date:	51
Access Layer Switch replacement % completion:	**~7%**
Total Distribution Layer Switches (UNMH, HSC):	41
Total Access Layer Switches replaced to date:	28
Distribution Layer Switch replacement % completion:	**~68%**

Recognition

- HSO ISO & Cyber Security team for outstanding teamwork

1) **Security** first, then everything follows.

2) **Cloudification** with an emphasize on storage, backup and recovery.

3) **Service Delivery** from our customers’ perspective.

4) **Collaboration** with Microsoft 365 adoption.

5) **Network Modernization** 1st year of a 5-year transformation journey.

18-Month Strategic Roadmap

Marquez
Microsoft 365

1. ~~Transfer domains~~
2. ~~Data migration~~
3. ~~Test~~
4. Training & Support
5. ~~Archived Termed EE~~

Meyer
Cyber Security

1. ~~6 KPIs~~
2. Azure MFA
3. RCA process
4. Vulnerability Assess
5. Phishing program
6. CMMC framework

Weaver
Network Redesign

1. ~~Requirements~~
2. ~~Network architect~~
3. Phase 1 of 3 in prog
4. KPIs
5. Staff development
6. ~~Upgrade Internet~~

Adcock
IT Service Management

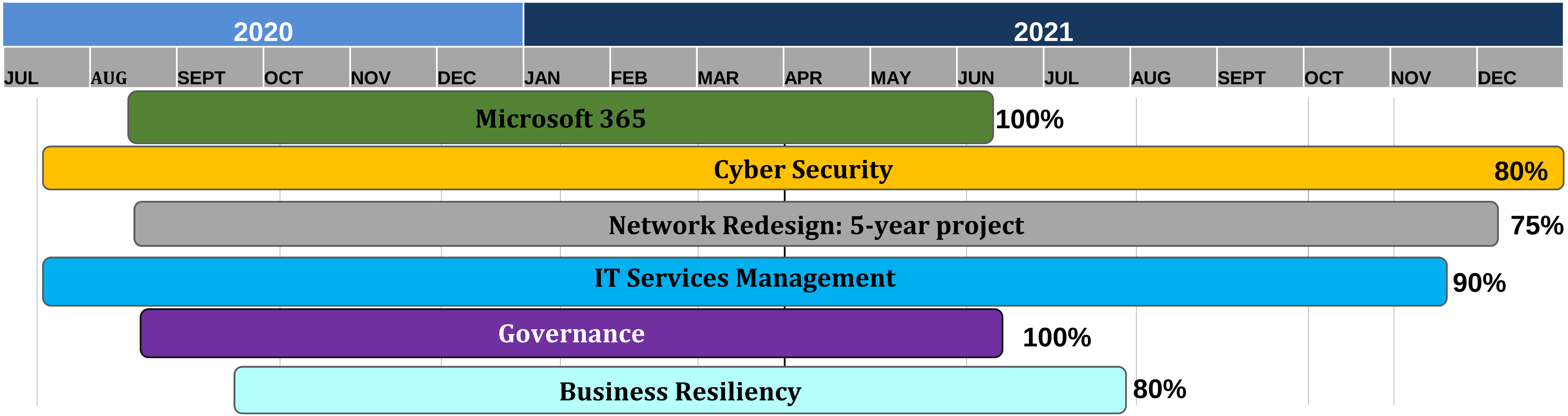
1. ~~4 KPIs Dashboard~~
2. ~~Aging tickets Rpt~~.
3. ~~Service Recovery~~
4. ~~Remote sup. tool~~
5. NPS survey
6. Single service portal

Sletten
Governance/Policies

1. ~~Charter for EIGC~~
2. ~~Policy Manager~~
3. ~~IT Website upgrade~~

Marquez
Business Resiliency

1. Storage upgrade
2. Backup/Recovery


JUL
AUG
SEPT
OCT
NOV
DEC
JAN
FEB
MAR
APR
MAY
JUN
JUL
AUG
SEPT
OCT
NOV
DEC
Microsoft 365
Cyber Security
Network Redesign: 5-year project
IT Services Management
Governance
Business Resiliency