SAMPLE POOL DIGITAL STRATEGY ROADMAP

POOL STRATEGY GUIDEPOSTS

- **Guidepost 1:** We will automate claims intake and underwriting renewal processes to decrease time to complete.
- **Guidepost 2:** We will improve our online member portal so that most of our members use it for baseline transactions with us.
- **Guidepost 3:** We will improve our culture so that most employees seem eager instead of fearful when it comes to new technologies.
- **Guidepost 4:** We will improve the digital skills of new team members with more robust technology onboarding.
- **Guidepost 5:** We will improve our cybersecurity defense capabilities by dedicating specific and accountable staff to the effort.

MAINTENANCE AND UPGRADES

Rationale: We view maintenance and upgrades to our software, systems and infrastructure as mandatory. We want all our systems up-to-date for security reasons — but also to make sure we use our tools most efficiently and can operationalize resources most effectively. The better we operate our systems, the better we can be for members.

Current Status: Many existing applications are out of date because we've heavily customized them, thereby making upgrades and updates difficult to implement. It's hard to schedule upgrades and updates because our internal work cycles (member renewals, claims processes, member response protocols, etc.) leave little room for scheduled downtime.

Improvements Needed:

- Focus on maintenance and upgrades as parallel efforts to other business priorities
- Carefully plan maintenance and upgrades around renewal schedules, and stick to the plan
- Create specific maintenance and upgrade budget line items to ensure proper and dedicated resource allocations are in place for this work
- Define associated risk and opportunity costs for each effort

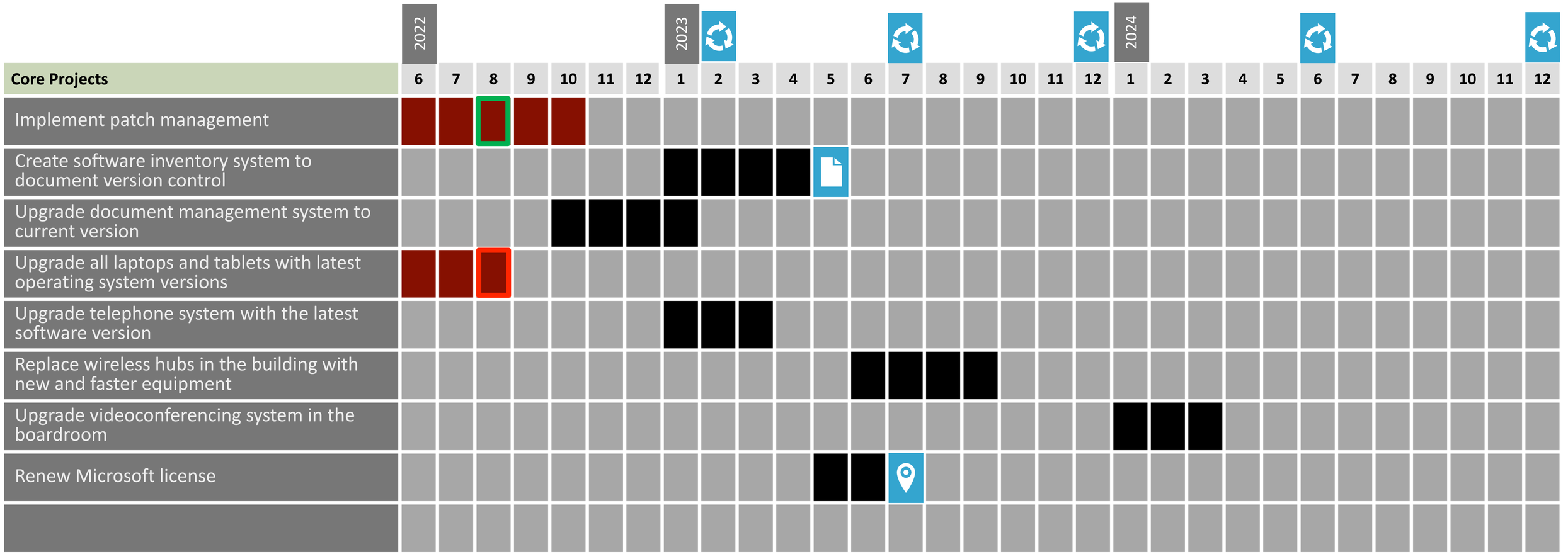
GOALS FOR MAINTENANCE AND UPGRADES

1. Create an annual schedule of maintenance and upgrades that won't interfere with renewal schedules.
2. Avoid security incidents that could be caused by lack of maintenance or patching.
3. Application versions are fully up to date.
4. The pool is aware of and can plan for upgrade schedules and feature additions being made by vendors.
5. Any decisions to skip or delay maintenance or upgrades are documented.

KPIS FOR MAINTENANCE AND UPGRADES

- Releases and upgrades are discussed in monthly management meetings and then scheduled.
- Upgrade implementations have a 90 percent or better success rate.
- There are no security incidents at the pool resulting from lack of patches, routine maintenance or upgrades.
- Maintenance costs do not increase more than 2 percent a year.

CORE PROJECT PLAN FOR MAINTENANCE AND UPGRADES



GUIDEPOST 1 We will automate claims intake and underwriting renewal processes to decrease time to complete.

GUIDEPOST 2 We will improve our online member portal so that most of our members use it for baseline transactions with us.

GUIDEPOST 3 We will improve our culture so that most employees seem eager instead of fearful when it comes to new technologies.

GUIDEPOST 4 We will improve the digital skills of new team members with more robust technology onboarding.

GUIDEPOST 5 We will improve our cybersecurity defense capabilities by dedicating specific and accountable staff to the effort.

ON TIME AND RUNNING SMOOTHLY

IN DANGER OF FALLING BEHIND

BEHIND SCHEDULE, COULD CREATE PROBLEMS

INNOVATION PROJECT

PROOF OF CONCEPT/ DISCOVERY

SECURITY ASSESSMENT

CONTRACTUAL COMMITMENT

DOCUMENT/ REPORT

STRATEGY DEVELOPMENT

ROADMAP REFRESH

MAJOR MILESTONE

NARRATIVE FOR MAINTENANCE AND UPGRADES

We want to limit our customizing of core systems in ways that freeze us out from future upgrades. We have struggled in the past with who owns this dimension, so we have assigned this dimension to a combination of our outsourced IT vendor and our administrative coordinator.

- The patch management software install is a baseline requirement and our top priority.
- The software inventory and maintenance cost process will be done on a spreadsheet that is shared with leadership annually.
- Maintenance agreements and pricing will be approved by the executive director so there is organization-wide understanding and visibility.
- The three version upgrade projects listed will be done by the IT vendor. We have already budgeted and scheduled these.

STAFF TRAINING

Rationale: Technology is just a large and complex set of tools. Without people who can use and improve these tools, we are wasting resources. We know that having a staff trained and talented in technology will improve our efficiency and boost how effective we can be for our members.

Current Status: We haven't invested in technology training across all staff. We don't hold our staff accountable for being fully literate in the technology tools we provide — "good enough" is sufficient, even though it shouldn't be.

Improvements Needed:

- Conduct technology training when onboarding new staff
- Provide ongoing technology training for existing staff
- Provide and require improved training when new systems are implemented
- Provide training on general skills like Microsoft 365 and Zoom
- Implement accountability measures for all staff to be trained and effective users of the technology tools appropriate for their work

GOALS FOR STAFF TRAINING

1. Create a technology training list by department and by role.

2. Create a structured onboarding process for new hires that includes introduction to technology resources and training on core technology for each role.

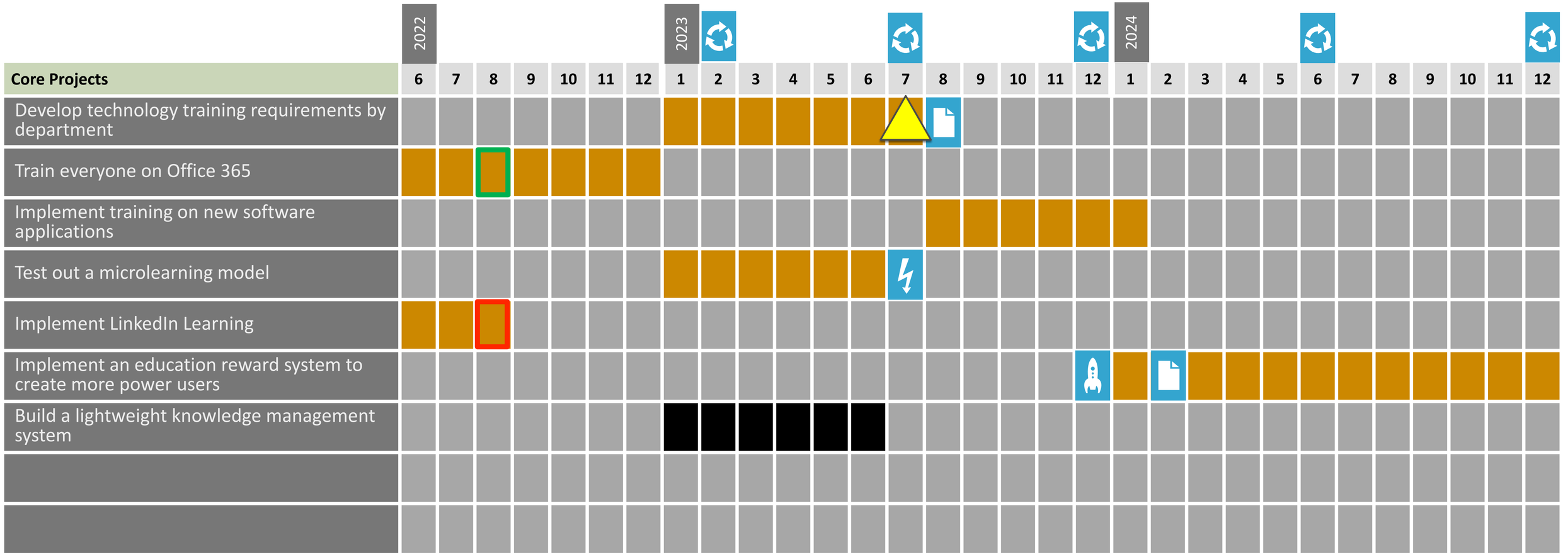
3. Implement an ongoing technology training program to keep staff current on all applications and processes.

4. Leaders set the example for the importance of making effective and efficient use of technology resources.

KPIS FOR STAFF TRAINING

- New hires test at or above 80 percent technology skills proficiency within four months of hire.
- Every employee has a performance measure related to technology training and skills, and everyone receives at least a “meets expectations.”
- New software implementations are rolled out with micro-learning modules, and all users are required to show completion of all modules.

CORE PROJECT PLAN FOR STAFF TRAINING



GUIDEPOST 1 We will automate claims intake and underwriting renewal processes to decrease time to complete.

GUIDEPOST 2 We will improve our online member portal so that most of our members use it for baseline transactions with us.

GUIDEPOST 3 We will improve our culture so that most employees seem eager instead of fearful when it comes to new technologies.

GUIDEPOST 4 We will improve the digital skills of new team members with more robust technology onboarding.

GUIDEPOST 5 We will improve our cybersecurity defense capabilities by dedicating specific and accountable staff to the effort.

ON TIME AND RUNNING SMOOTHLY

IN DANGER OF FALLING BEHIND

BEHIND SCHEDULE, COULD CREATE PROBLEMS

INNOVATION PROJECT

PROOF OF CONCEPT/ DISCOVERY

SECURITY ASSESSMENT

CONTRACTUAL COMMITMENT

DOCUMENT/ REPORT

STRATEGY DEVELOPMENT

ROADMAP REFRESH

MAJOR MILESTONE

NARRATIVE FOR STAFF TRAINING

This dimension might be one of the easiest to deliver on, but it is also the first one that gets pushed to the side to meet other priorities. We know we have to commit to digital education to meet our goals.

- We have experienced that new people are taking too long to get up to speed on our digital tools.
- We made the mistake of not training intensively enough when we implemented new technology, but we will not do that from now on.
- Incentivizing “power users” will encourage people to self-learn tools.
- LinkedIn Learning is an inexpensive way to bring lots of digital courses to our team and requires two fundamental steps: 1) purchase the system and 2) get people to take the needed courses.

DIGITAL GOVERNANCE

Rationale: Establishing written policies and practices about roles and accountabilities for our technology is important to protect our systems and improve our operations. We want expectations to be clear and changes to be communicated well. Strong digital governance is important to everything else we're trying to accomplish with our digital strategy.

Current Status: We experience a fair amount of internal friction and disruption when implementing and using new digital systems. There's inconsistency and lack of common understanding about whether business or technology interests drive new initiatives. When we make changes to technology, we don't always communicate effectively.

Improvements Needed:

- Have the business side of our operation drive tech changes (exception: network and system security)
- Develop guidelines about how to use existing or new applications
- Create standardized controls for how new solutions are implemented and how systems are decommissioned
- Create standards for appropriate use of pool technology
- Focus on governance that helps with cyber risk control

GOALS FOR DIGITAL GOVERNANCE

1. We have an ABO (application business owner) for every software tool we use.

2. All core business and workflow processes, policies and procedures are fully documented, including how and where software applications are utilized to support workflow.

3. Our data and security governance lowers risk levels for the pool.

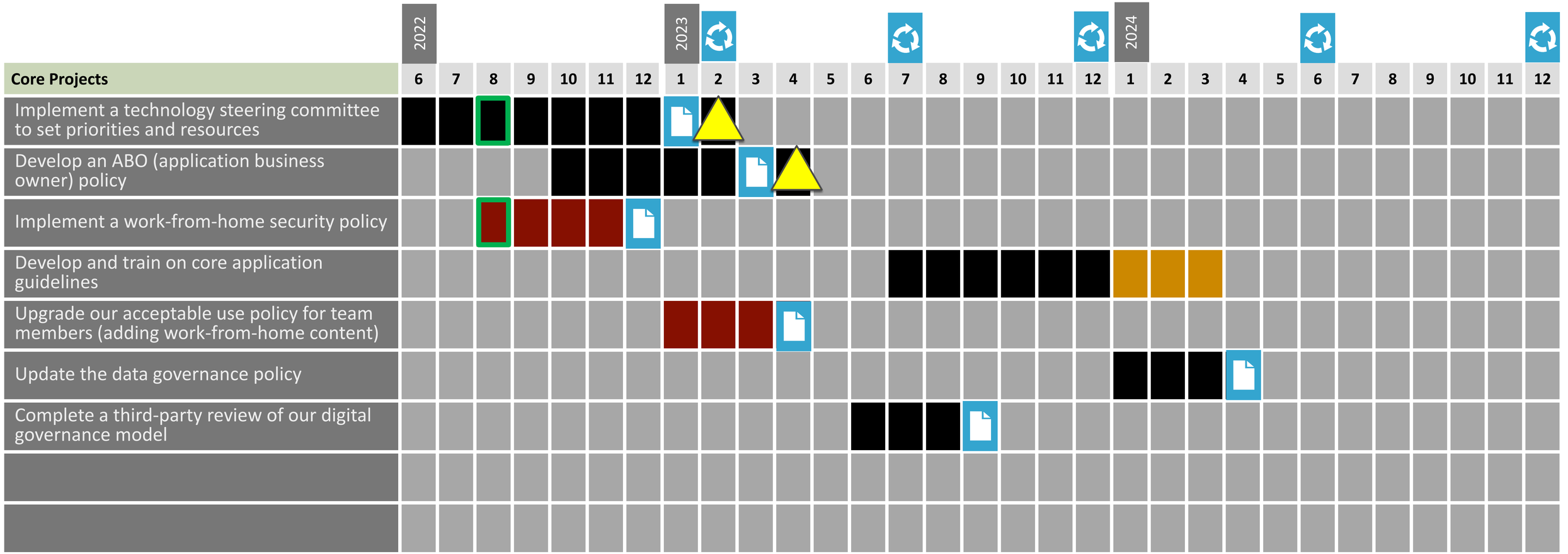
4. Everyone knows our digital priorities.

5. Staff understand allowable use of pool technology and tools.

KPIS FOR DIGITAL GOVERNANCE

- There is a complete, fully current application inventory that connects software tools to workflow and business processes.
- A written technology use policy has been agreed to by all staff and has been added to staff onboarding education.
- When surveyed informally in meetings or conversations, all staff can accurately name at least half of our current digital priorities.
- The governing body has received a list of our digital priorities.

CORE PROJECT PLAN FOR DIGITAL GOVERNANCE



GUIDEPOST 1 We will automate claims intake and underwriting renewal processes to decrease time to complete.

GUIDEPOST 2 We will improve our online member portal so that most of our members use it for baseline transactions with us.

GUIDEPOST 3 We will improve our culture so that most employees seem eager instead of fearful when it comes to new technologies.

GUIDEPOST 4 We will improve the digital skills of new team members with more robust technology onboarding.

GUIDEPOST 5 We will improve our cybersecurity defense capabilities by dedicating specific and accountable staff to the effort.

ON TIME AND RUNNING SMOOTHLY

IN DANGER OF FALLING BEHIND

BEHIND SCHEDULE, COULD CREATE PROBLEMS

INNOVATION PROJECT

PROOF OF CONCEPT/ DISCOVERY

SECURITY ASSESSMENT

CONTRACTUAL COMMITMENT

DOCUMENT/ REPORT

STRATEGY DEVELOPMENT

ROADMAP REFRESH

MAJOR MILESTONE

NARRATIVE FOR DIGITAL GOVERNANCE

We will make a concerted effort to upgrade our digital governance in a few key areas. We have studied the digital governance models at other pools and discussed what is reasonable for our pool size.

- The technology steering committee will bring together people from every department to be involved with resources and priorities.
- Application business owners will help us make better software and data decisions and make clear who has responsibility for our software tools.
- The work-from-home (WFH) security policy will help us close the security holes we have now with our hybrid team.
- Data governance will ensure we do not have inordinate risks of data loss due to poor data handling practices.

DATA ACTIVATION

Rationale: Data is gas to the engine of our pool's digital strategy and infrastructure. Being able to unlock the value in data requires developing insights from information and then acting on those insights in meaningful ways.

Current Status: We have data in silos that are not fully accessible to everyone. This limits our reporting and analytics capabilities because we cannot correlate data points and make true analytical sense of our robust information sources.

Improvements Needed:

- Better direct availability of existing reports and easier methods to share reports (internally and externally)
- Ability to report on any custom fields created in our core systems
- Tools to identify correlations we might not otherwise know exist (e.g., factors influencing the cost of a claim)
- Improved data aggregation, integration and organization methods

GOALS FOR DATA ACTIVATION

1. We have a single system of record for member and contact information that is accessible and used by everyone (for every function).

2. Any data field captured in any system can be reported on, and we can correlate data between systems when useful.

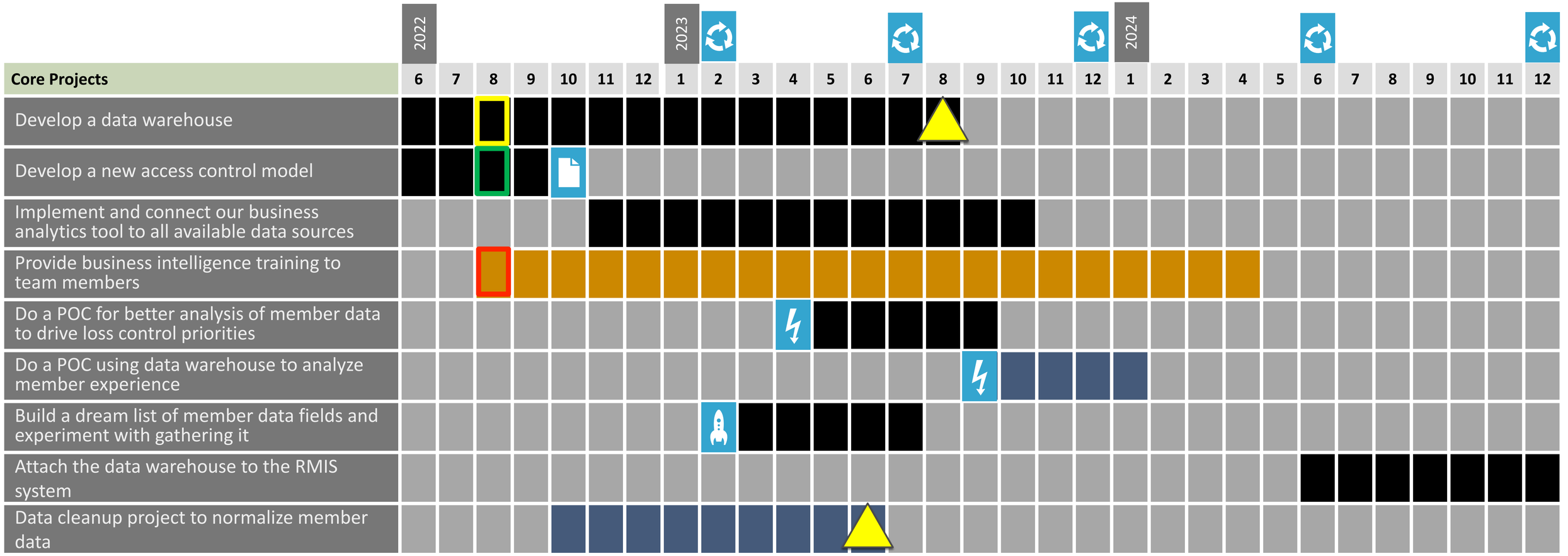
3. We use predictive analytics tools to look for correlations that impact claim outcomes.

4. There are descriptive dashboards in place to illustrate the risk at the member level and on the whole of the pool.

KPIS FOR DATA ACTIVATION

- Member and contact data redundancy has been eliminated, and we have all required fields of data for members.
- All of our employees are trained on ad-hoc reporting.
- We have developed and implemented claims assignment and management processes to match the outcome correlations generated by our analytics.
- Half of our members have accessed descriptive dashboards.

CORE PROJECT PLAN FOR DATA ACTIVATION



GUIDEPOST 1 We will automate claims intake and underwriting renewal processes to decrease time to complete.

GUIDEPOST 2 We will improve our online member portal so that most of our members use it for baseline transactions with us.

GUIDEPOST 3 We will improve our culture so that most employees seem eager instead of fearful when it comes to new technologies.

GUIDEPOST 4 We will improve the digital skills of new team members with more robust technology onboarding.

GUIDEPOST 5 We will improve our cybersecurity defense capabilities by dedicating specific and accountable staff to the effort.

ON TIME AND RUNNING SMOOTHLY

IN DANGER OF FALLING BEHIND

BEHIND SCHEDULE, COULD CREATE PROBLEMS

INNOVATION PROJECT

PROOF OF CONCEPT/ DISCOVERY

SECURITY ASSESSMENT

CONTRACTUAL COMMITMENT

DOCUMENT/ REPORT

STRATEGY DEVELOPMENT

ROADMAP REFRESH

MAJOR MILESTONE

NARRATIVE FOR DATA ACTIVATION

There are two elements to our data activation projects that are important to meet the goals we have set for this dimension. The first is implementing new software tools. The second is growing the data skills of our team members.

- The pool has talked about a data warehouse for a long time. Our data is spread across many systems, and it is difficult to mine useful perspective.
- We also need better tools for doing analytics and data visualization.
- The proof of concept (POC) projects are important because they will teach the pool important lessons about activating data in two of our most critical areas.
- Business intelligence training within every pool function is crucial because all the technology in the world will not matter if our people cannot pull the value from the data sources they have.

CYBERSECURITY

Rationale: Today's cyber risk environment is dynamic, and threats come from many sources at a rapid pace. Aside from core business risks that come from a breach in our cybersecurity, there could also be significant reputational harm to the pool if our systems or data were compromised.

Current Status: We aren't large enough to have full-time cybersecurity experts on staff. We have contracted resources but no good way to evaluate the quality of their work. We spend more time and effort on addressing the cybersecurity needs of members than of our own operations.

Improvements Needed:

- Get third-party help with monitoring for and response to attacks — we need to feel fully confident in the vendor we choose to do this work
- Be more intentional about identifying our cyber risks — create a cyber incident response plan for our pool
- Improve the quality and quantity of cyber training for all staff

GOALS FOR CYBERSECURITY

1. Implement a managed detection and response system in order to respond to threats in under five minutes.

2. The standards and protocols to report cybersecurity events are understood by all staff (as is the definition of “event”).

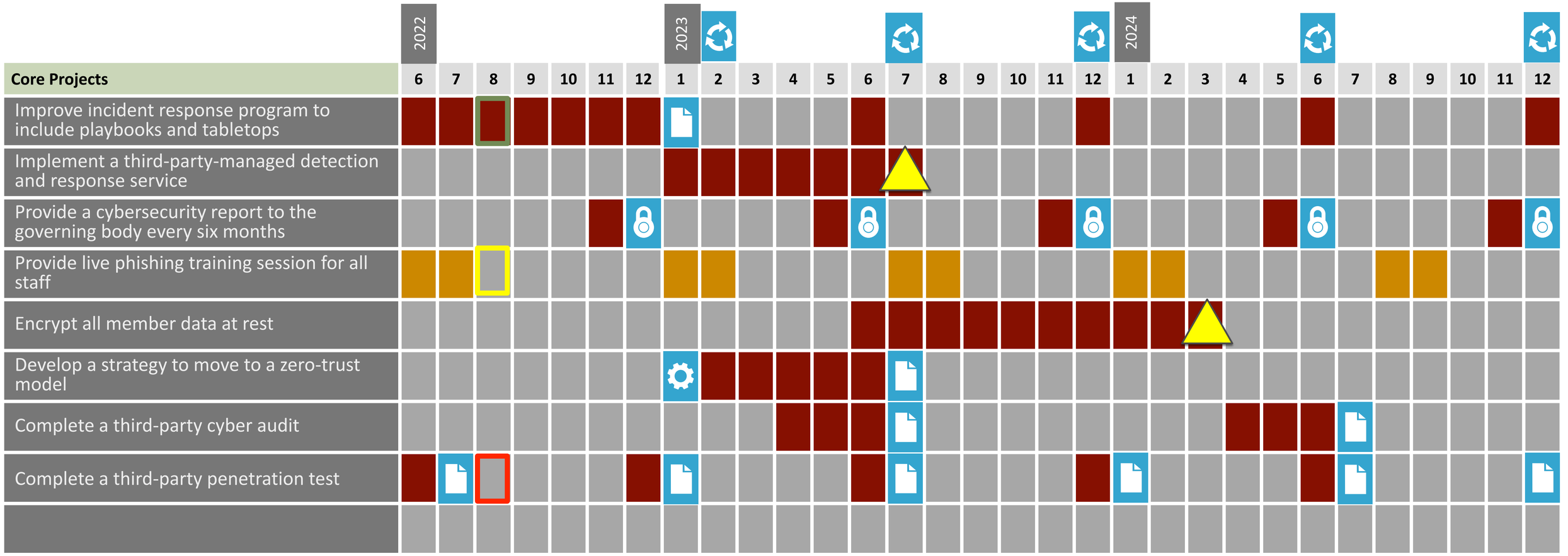
3. Upgrade our cyber incident response plan (CIRP) so that it is acceptable to our regulators.

4. Use multi-factor authentication (MFA) for email, logging into to the network remotely, and logging into operational systems remotely.

KPIS FOR CYBERSECURITY

- Our annual cyber audit does not identify any unaddressed risk areas.
- Our annual CIRP tabletop exercise indicates no needed changes to our plan.
- Phishing and social engineering testing for staff results in no failed responses.

CORE PROJECT PLAN FOR CYBERSECURITY



GUIDEPOST 1 We will automate claims intake and underwriting renewal processes to decrease time to complete.

GUIDEPOST 2 We will improve our online member portal so that most of our members use it for baseline transactions with us.

GUIDEPOST 3 We will improve our culture so that most employees seem eager instead of fearful when it comes to new technologies.

GUIDEPOST 4 We will improve the digital skills of new team members with more robust technology onboarding.

GUIDEPOST 5 We will improve our cybersecurity defense capabilities by dedicating specific and accountable staff to the effort.

ON TIME AND RUNNING SMOOTHLY

IN DANGER OF FALLING BEHIND

BEHIND SCHEDULE, COULD CREATE PROBLEMS

INNOVATION PROJECT

PROOF OF CONCEPT/ DISCOVERY

SECURITY ASSESSMENT

CONTRACTUAL COMMITMENT

DOCUMENT/ REPORT

STRATEGY DEVELOPMENT

ROADMAP REFRESH

MAJOR MILESTONE

NARRATIVE FOR CYBERSECURITY

We know our cybersecurity defenses are not strong enough in today's environment of constant and changing threats. We have delayed doing a few of the tasks needed because of costs. We can no longer do this and have the approval of our governing body for improvements.

- Building an incident response system and periodic tabletop exercises will help us respond expertly if a successful event does happen.
- Engaging third parties for penetration testing and cyber audits will help us ensure that our security risk level is where our governing body wants it to be.
- The combination of better security training, new governance policies and phishing testing will help us lower the "human firewall" risk.
- Encrypting member data at rest will ensure that, if our network ever gets penetrated, the loss of data will be minimum.

ENVIRONMENTAL FACTORS SCORER

#	ENVIRONMENTAL FACTOR	POOL READINESS SCORE	FACTOR WEIGHT	FACTOR ALARM	INDIVIDUAL SCORE-TO-WEIGHT RATIO
1	Resource Availability	8	10		50%
2	Motivation and Will	6	8		50%
3	Digital Skills and Knowledge	4	9	Needs Attention	50%
4	Key Opinion Leaders Buy-In	6	8		50%
5	Digital Culture	5	6		50%
6	Resource Availability	4	9	Needs Attention	50%
7	Working Environment	5	7		50%
8	Pace of Change Tolerance	3	8	Needs Attention	50%